Health Information Security and Privacy Collaboration
Phase Two

State Implementation Project Summary and Impact Analysis Report

Arizona Health Privacy Project

Prepared by:

Arizona Government Information Technology Agency
100 North 15th Avenue, Suite 440
Phoenix, Arizona 85008

Coppersmith Gordon Schermer Brockelman, PLC
2800 North Central Avenue, Suite 1000
Phoenix, Arizona 85004-1008

Submitted to:
Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange
Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

Table of Contents

Executive Summary

Arizona Health-e Connection (AzHEC) is a non-profit organization formed in 2007 to implement Health Information Exchange (HIE) and the deployment of Health Information Technology (HIT) in Arizona. To accomplish its goals of improving the quality and decreasing the costs of health care in Arizona, AzHEC is working closely with the following initiatives in Arizona: (1) The Arizona Health Care Cost Containment System (AHCCCS, Arizona's Medicaid program) Health Information Exchange and Electronic Health Record (HieHR) Project; (2) the Southern Arizona Health Information Exchange (SAHIE); and (3) the GITA Rural Health Information Technology Grant Program.

To support the work of these organizations, the Arizona Health Privacy Project (AHPP) has completed a great deal of work to study and implement private and secure health information exchange in Arizona. In Phase One of the HISPC Project, AHPP reviewed the variations in business practices relating to the sharing of electronic health information across Arizona. AHPP then determined which business practices were barriers to health information exchange and designed potential solutions to those barriers. During the implementation planning in Phase One, AHPP focused its implementation plans on access and authentication of the provider to access HIEs and began the work of designing legislative and regulatory solutions to removing potential barriers to HIE in Arizona.

Under Phase Two of this project, the AHPP team has convened a wide range of stakeholders to continue implementation of these challenging projects. The team approached implementation of these goals from two perspectives: a functional / technical approach and a legal approach. Because there are no operational HIEs in Arizona yet, we chose the HIE model closest to implementation on which to base our work: the AHCCCS HieHR project, which is scheduled for pilot implementation in June 2008.

Functional/Technical Work: The functional / technical approach to this project involved developing an access and authentication approach for providers to access an HIE. The Functional / Technical Working Group (FTWG) held working sessions on a weekly basis and shared the results with stakeholders as research was completed. We conducted extensive research on national standards for authentication and interviewed existing HIEs to see how they are handling authentication. The AHPP identified significant potential solutions, all of which pose challenges that need to be resolved:

1) Public Key Infrastructure (PKI), a standard for strong authentication, can be deployed uniformly across multiple RHIOs but has substantial limitations including uncertain certificate revocation, conditions for certificate issuance and reliance, variability of regulations and evidentiary laws by jurisdiction, and trust.

2) Digital Signatures can be used to authenticate the source of a message but also has the limitation the user can only sign documents on a particular computer (unless the individual has a smart card that allows the use of the private key on any computer) and the security of the private key completely depends on the security of the computer, which is notoriously unreliable for many PCs and operating systems.

3) Biometrics can be used, but can be slow and expensive to implement and use if there are large number of users.

4) Security tokens are viable for HIEs, but pose distribution difficulties and expense.

5) Two-factor ("something you know plus "something you have" or "something you are" is a secure method of authentication, but pose challenges to interoperability across organization and increase the costs of authentication.

6) "Local" registration and enrollment through participating entities is viable for larger scale deployments to provide strong authentication, although establishing an enrollment strategy and process takes considerable time to formulate and implement. The biggest challenge is to ensure a smooth, manageable (and ideally, automated) enrollment process for both the healthcare organization and the practitioner.

7) The National Provider Identifier (NPI) cannot be used as the sole method of identifying a provider, because it does not determine whether applicants are licensed providers, and applicants can have more than one NPI. The Arizona health profession regulatory boards will be better sources for determining an applicant is a licensed health care provider.

The AHPP will continue to work on choosing a technical solution that is easy to implement and user-friendly. We will continue to work with the stakeholder community and the newly formed Arizona Health-e Connection Consumer Advisory Council. We will also continue to research cost and feasibility of PKI and two-factor authentication as well as automating the method of registering all providers and looking at how we can achieve single sign-on. We will recommend to the Arizona Health-e Connection Board of Directors to complete a risk assessment as recommended by the HIMMS / GSA e-Authentication Project Whitepaper.

Legal Work: In Phase Two of the HISPC project, the Legal Working Group is developing a model participation agreement and model policies and procedures for HIEs in Arizona. This legal work is essential to facilitate development of HIEs in Arizona, and the sharing of health information among those HIEs, developing in Arizona, where consistent privacy and security processes and policies are important to achieve "policy interoperability." The LWG held multiple meetings and formed a "Best Practices Subgroup," which researched fourteen developing HIEs across the country to gather information on core policies (such as patient consent) and sample agreements.

The Legal Working Group also has developed proposed statutory and regulatory amendments. First, the LWG developed proposed amendments to statutes regarding information regarding communicable disease, mental health, immunization, and genetic testing, and subpoenas for medical records, to remove the barriers to electronic exchange of health information within an appropriate privacy and security framework. The LWG also has worked on developing a comprehensive enforcement and consumer rights framework, and the entire legislative package will be introduced in January 2009. This timeline will allow Arizona Health-e Connection time to work with stakeholders and the Arizona legislature in advance, so that we can address potential concerns to the legislative package in advance of the session.

The Legal Working Group conducted multiple meetings and is doing additional outreach to stakeholder groups to refine the work products. The LWG also will be working with the Arizona Health-e Connection Consumer Advisory Board to involve consumers in important policy decisions regarding HIE operation.

Multi-State Collaborative Work: The AHPP has developed a proposal to receive funding to be a part of the Standards Collaborative to address audit, provider identification (access and authentication) and patient identification to allow interoperability across states to share electronic health information. This proposal effort was co-chaired by Kim Snyder. Kristen Rosati will be chairing the legal team working on this effort as well. Arizona is working with Connecticut, Colorado, Utah, Washington, Virginia, Maryland, Oklahoma, Nebraska and Ohio.

Introduction and Overview

Arizona Health-e Connection (AzHEC):

Arizona Health-e Connection (AzHEC) is a non-profit organization formed in 2007 to implement Health Information Exchange (HIE) and the deployment of Health Information Technology (HIT) in Arizona, striving to improve the quality and decrease the costs of healthcare in Arizona. AzHEC originated from an executive order by Governor Napolitano, which established a steering committee to oversee the development of a comprehensive statewide roadmap and subsequent implementation activities involving hundreds of individuals and organizations throughout Arizona. The Arizona Health-e Connection Roadmap was published in 2005.

The Roadmap:

- Encouraged health information technology adoption among health care providers;
- Identified key infrastructure components that enable providers to securely exchange health information; and
- Encouraged the development of a not-for-profit, public-private governance organization with representation from all major stakeholders groups to provide leadership implementing the Roadmap

The not-for-profit organization—Arizona Health-e Connection—was formed, with a broad array of private and public stakeholders. To implement the Roadmap, AzHEC has identified the following strategic initiatives:

1) Education and Outreach: AzHEC seeks to provide a single source of information about health information technology (HIT) adoption and health information exchange (HIE) and coordinating "messaging" with developing HIEs across the state.
2) Establishing Statewide Standards, Policies and Legal Agreements: Primarily through the HISPC Grant awarded to the State of Arizona, AzHEC is working on standards for technology, as well as creating standardized legal agreements for participating in the HIEs and the policies for HIEs in Arizona. The HISPC Grant also has funded the legal work to identify statutory and regulatory changes needed to facilitate HIE in Arizona.
3) Support of Health Information Exchange Infrastructure: AzHEC may also seek to create statewide technology infrastructure to achieve interoperable health records and HIE, while providing support and coordination to the Medicaid HIE being established the Arizona Health Care Cost Containment System (AHCCCS) and the Southern Arizona Health Information Exchange (SAHIE). The Roadmap suggested development of regional infrastructure, with exchange facilitated between regions, and to develop state-level infrastructure when it is deemed most efficient and cost effective.

To accomplish these goals, AzHEC is working closely with the following initiatives in Arizona: (1) The Arizona Health Care Cost Containment System (AHCCCS) Health Information Exchange and Electronic Health Record (HieHR) Project; (2) the Southern Arizona Health Information Exchange (SAHIE); and (3) the GITA Rural Health Information Technology Grant Program.

AHCCCS Health Information Exchange and Electronic Health Record (HieHR) Project: Funded by the Centers for Medicare and Medicaid Services (CMS) through a Medicaid Transformation Grant, this $12 million effort will provide an HIE for AHCCCS providers. In its second phase, the project will also provide an electronic health record (EHR) for AHCCCS providers, reaching more than 1.1 million Arizona citizens currently on Medicaid.

Because HIEs are still developing throughout Arizona, we utilized the proposed AHCCCS model for HIE (as shown in Figure one) as the model for the Arizona Health Privacy Project work to support the development of HIEs in Arizona. The proposed method for authenticating providers, who are licensed and affiliated with a participating entity, to the HIE is shown in figure 2. The AHCCCS infrastructure model permits providers to access limited information—medication history, labs, hospital discharge summaries, and advance directives—through a Web viewer, using a record locator service (as shown in Figure three).

Figure 1. Architecture of Phase I AHCCSCS HieHR Project

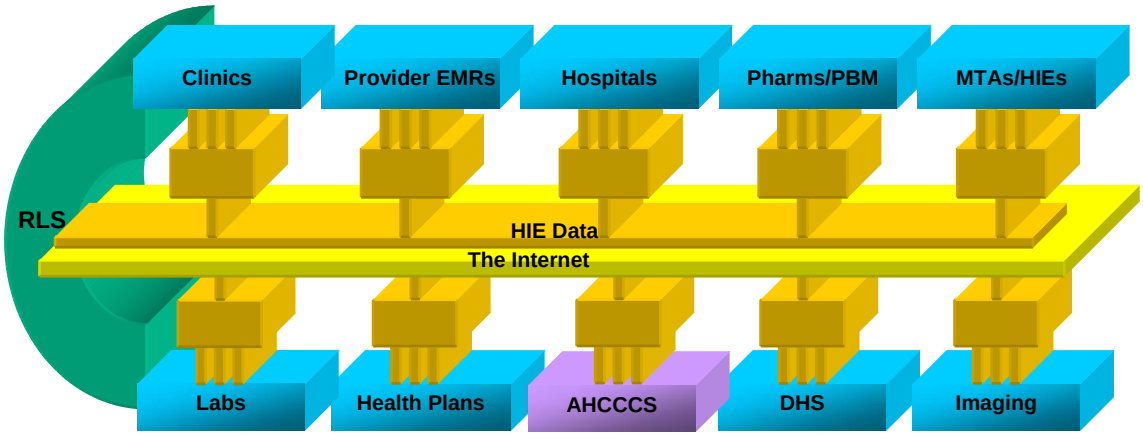


Figure 1: This represents Phase I of the HIE that AHCCCS will implement as a pilot project with hospital discharge summaries from three hospitals, laboratory results from two commercial clinical laboratories, medication history from SureScripts and RxHub, and advance directives from the State of Arizona. Providers will be able to access this limited clinical information through a Web-based Viewer. The system will utilize a Record Locator Service to match patient records, and will authenticate the users and create audit logs of access.

Figure 2. Proposed Flowchart of method for adding participating entities to the HIE:

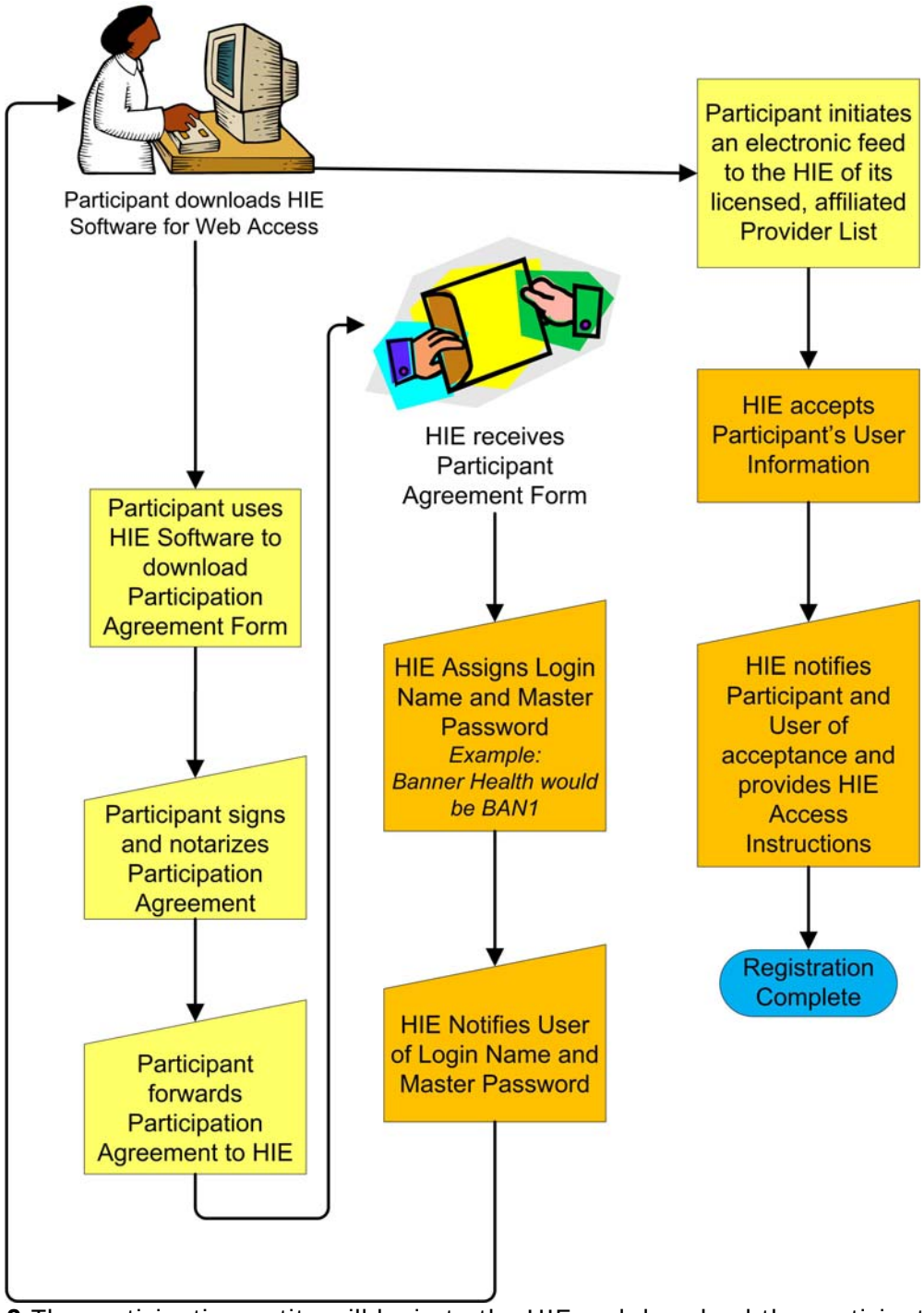


Figure 2. The participating entity will login to the HIE and download the participation agreement, sign, notarize and fax it back the HIE. The HIE will then issue a login and password to the participating entity. The participating entity will then provide the HIE with a list of authorized users who are licensed and affiliated with that participant; the HIE will notify the participant of acceptance and instructions to login to the HIE. (note: this does not cover providers who are not affiliated with an entity or providers who are not licensed.)

Figure 3. Data Flow from the HIE to the Provider

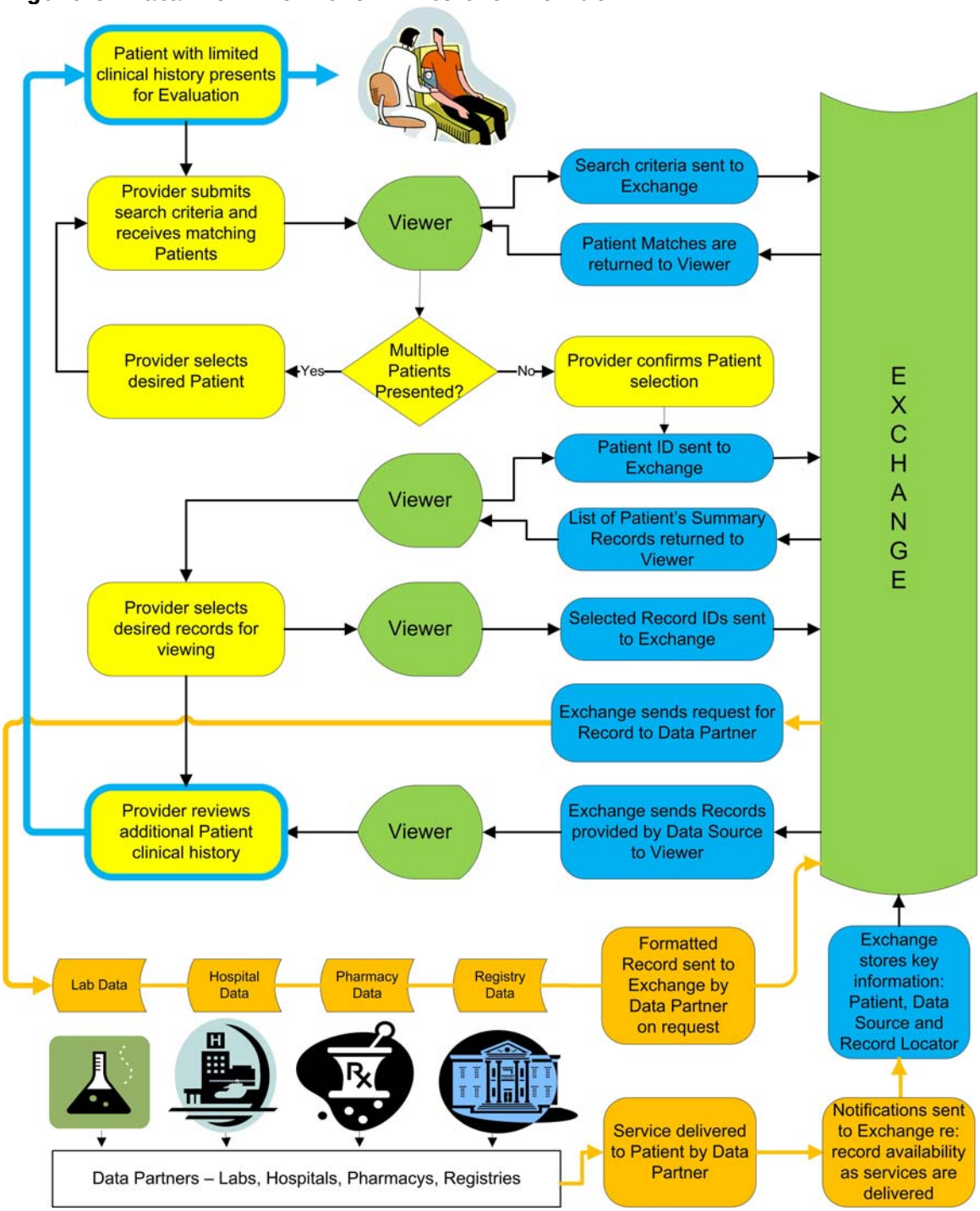


Figure 3. The information that will be available to providers in the first phase of the project will include medication history, lab test results, discharge summary and advance directives. When the patient presents to the provider, the provider can log into the HIE and submit search criteria. The HIE pulls potential patient matches, and the provider can then select the desired patient. The HIE then presents a list of records available to the provider, which the provider may select.

Southern Arizona Health Information Exchange (SAHIE): The mission of this private, multi-stakeholder organization is to facilitate the exchange of health information between Southern Arizona providers and provide EMRs to providers. The Southern Arizona Health Information Exchange (SAHIE) is a community-driven project to create an HIE in the Medical Service Area around Tucson. The project is funded by a consortium of 14 organizations, including healthcare payers, all rural and urban hospitals in the area, the major group practices and Community Health Centers. The project is being conducted in phases. In the current phase, the objectives are to design the organizational structure for this non-profit; to determine the detailed design and vendors for the product, and make an implementation plan to start in July 2008. SAHIE is coordinating closely with AzHEC, AHCCCS, and any other HIEs that develop in the state.

The GITA Rural Health Information Technology Grant Program: Governor Napolitano established a $1.5 million Rural Health Information Technology Adoption Grant Program, and the program is well underway. Seven rural Arizona health care providers have been awarded grants, most of which has been used in collaborative efforts. A second round of grants will be made to provide health information technology and health information exchange consulting expertise and funding to rural areas. This grant will provide rural Arizona leadership with access to "best in class" consulting expertise for consideration of their own health information exchange, or to further leverage the investment of an existing health information exchange, such as SAHIE.

AzHEC, AHCCCS and SAHIE are all working on two fronts. First, they are working to assist clinicians and other health care providers implement EMRs and other health information technology (HIT) in their practices and businesses to help them meet their clinical and business needs. From a technology adoption perspective, Arizona's health care providers mirror adoption rates in most other parts of the United States. Large hospitals and provider groups have adopted various forms of technology including electronic medical records and e-prescribing. Additionally, most labs and pharmacies have implemented technology to deliver services. However, it is estimated that only between 15% and 19% of small medical practices have implemented EMR. Second, AzHEC, AHCCCS and SAHIE are working collaboratively on encouraging HIE throughout the state.

Arizona Health-e Connection, GITA, SAHIE and AHCCCS staff are meeting and communicating daily, to ensure our efforts are coordinated. SAHIE and AHCCCS have seats on the Arizona Health-e Connection Board, while AHCCCS and Arizona Health-e Connection participate in the SAHIE Steering Committee. We are sharing best practices, and information gained from our interaction with other states, to ensure Arizona chooses the right path to achieving a complete health information infrastructure, resulting in higher quality care and patient safety, for all Arizonans.

Doctors Office Quality-Information Technology Program: The HISPC project team included the Project Director for the Arizona CMS-sponsored Doctors Office Quality-Information Technology (DOQ-IT) program. DOQ-IT worked with over one hundred practices to evaluate EHRs, negotiate contracts, implement and trouble shoot their EHRs, develop templates and reports with the physicians, and generate quality reports from their EHRs. Most of the physicians participating were either solo practitioners or in small to medium sized group practices. The software packages implemented were varied. Many of the EHR systems that are affordable to the small to medium sized physician office have cut corners in their program that need to be identified and stabilized in order for the physicians to truly be successful with their systems. Two examples of these corners include the use of drug databases without sufficient decision

support and the lack of ability to export an HL7 message from the clinical side of the system. This dramatically effects how these physicians will be able to participate in HIEs or RHIOs.

Implementation Project Update

During Phase One of the HISPC project, the Arizona Health Privacy Project (AHPP) Team worked with stakeholder groups to address variations in business practices among stakeholders and barriers to health information exchange in Arizona. The AHPP Team identified the following solutions to those barriers by classifying them into the following categories:

- Development of regional health information exchanges
- Solutions for authorization and authentication problems
- Solutions for secure information transmission or exchange
- Solutions to prevent unauthorized modifications
- Solutions for current paper-based systems, primarily focused on information exchange by fax
- Enhancing patient's role in controlling their personal health information
- Solutions affecting federal law/regulations

The AHPP Team then provided implementation plans to address these solutions. The implementation plans included:

- Research specific technology and process solutions for a state-level master provider index to serve as a clearinghouse for all RHIOs in the state
- Research specific technology and process solutions for authentication, authorization, access and audit
- Create education and outreach program
- Form a group to investigate state specific data element standards and oversee implementation of national level standards for electronic medical records
- Develop proposed amendments of statutes and regulations to facilitate e-health data exchange.

During the implementation planning, the AHPP Team reviewed other initiatives in the state that would be affected by the implementation planning. Since AHCCCS is planning to have its HIE functional and in pilot testing by June 2008, it was clear that the development of access and authentication functionality would assist AHCCCS and other developing HIEs. We also decided to develop the agreements needed for participants and entities to be authorized to access the HIE as, well as the policies and procedures for use of the HIE.

The AHPP Team has made significant progress to date in addressing access and authentication functionality, as well as development of the model policies and a model participation agreement, and in planning legislative and regulatory changes, as outlined below. We have divided the progress into two sections: Functional and Legal.

Progress of Functional Work:

The AHPP Functional / Technical Working Group (FTWG) has researched standards for access and authentication, as well as conducted research of other states' efforts to determine what methods may have been or are in process of being implemented to authenticate provider access to the HIE.

There are many types of standards to research when embarking on a health information exchange project. Some standards are necessary to ensure the privacy of the data that moves through the network (who has access and for what purpose), some standards help ensure that the security of the participant's network is adequate, and some standards ensure that the data elements are interoperable (or at least able to be mapped) so that the information exchanged is both human and machine readable.

The FTWG performed a literature review to determine the recommended national standards, conducted interviews to determine what standards other states are using, and then through the convening stakeholders, intends to identify the pros and cons of each standard. From this, the FTWG will identify and recommend the direction for Arizona. The FTWG researched the following standards:

(1) Transport standards determine how data is transmitted from one entity to another. For instance, the Health Level 7 (HL7) message standard is the standard for transporting clinical messages. Physician offices send their billing data in an HL7 message to their clearinghouses for payment. HL7 was given the ominous duty of identifying functional criteria that ambulatory and inpatient EHRs should be able to perform. In addition, HL7 provides a code set that can be used in determination of very granular role-based access to the HIE.

(2) Radiology images use DICOM as the transport standard when transmitting images between radiology PACS systems.

(3) SAML is an XML standard for communicating user authentication, entitlement, attribute information, and authorization data between security domains, an identity provider and a service provider. Many states are adopting this standard as they work toward a uniform provider identity.

(4) There are over 200 terminology standards in use today in the medical informatics community. Some of the more well-known terminology standards include ICD9 and CPT 4. Others include NDC for the national drug codes, also used in prescriptions, and LOINC codes for laboratory orders and results. Perhaps the clinical terminology with the most comprehensiveness and clinical value is SNOMED CT.

(6) The ASTM Continuity of Care Record (CCR) standard is a patient health summary standard, a way to create flexible documents that contain the most relevant and timely core health information about a patient, and to send these electronically from one care giver to another. It contains various sections -- such as patient demographics, insurance information, diagnosis and problem list, medications, allergies, care plan, etc. – that represent a "snapshot" of a patient's health data that can be useful, even lifesaving, if available when patients have their next clinical encounter. The ASTM CCR standard is designed to permit easy creation by a physician using an electronic health record software program (EHR) at the end of an encounter. The ASTM CCR standard combined with HL7 has allowed for a standard making clinical data transportable, this is called Continuity of Care Document (CCD).

(7) Security within a RHIOS or HIEs is one of the most critical components that must be implemented in such as way as to ensure confidentiality to the participants and integrity of the information exchanged. The General Services Administration

(GSA) approached the Healthcare Information and Management Systems Society (HIMSS) in 2005 to discuss partnering on a pilot project that would show the applicability of the federally adopted security technology and solutions for the healthcare information sharing. The pilot project utilized the GSA's e-Authentication Service Component program to provide digital certificates, technical architecture development support and certificate validation services. Six state projects are participating in the pilot: Connecticut (eHealthConnecticut), Michigan (Michigan Data Sharing & Transaction Infrastructure Project), Minnesota (Community Health Information Collaborative), Ohio (eHealth Ohio-OSC Bioinformatics), Ohio (Virtual Medical Network), and Texas (Christus Health, health eCities project). Although none of the pilots are actually exchanging data yet, much was learned regarding authentication and authorization. The registration process required Local Registration Authorities (a difficult process in and of itself) to physically go and register physicians, which turned out to be quite a logistical challenge.

(8) There are other types of standards such as those used for prescriptions used in e-prescribing systems, namely, NCPDP, and standards for medical devices (IEEE/CEN/ISO 1073). There are also various web-based standards, such as XML and SOAP; and administrative and finance standards, such as ANSI X12N.

The Clinical / Technical Committee of AzHEC is performing a research of other states to inquire about the functionality of their health information exchanges. The following questions were asked as they relate to access and authentication of provider access to the HIE:

1) Does the HIE have a provider index?
   If so, how is it maintained?

2) How does the HIE authenticate providers and where is it getting the provider information?

3) Do you have single sign-on for the providers to access the HIE?

Of the six HIEs we are investigating (Indiana Health Information Exchange, MA-SHARE, THINC, HealthBridge, MHIN, Inland Northwest Health Services), we have results from three at the time of this report. We found that:

- Single sign-on is provided at the web portal to the HIE;
- Hospitals and state agencies supply the providers and the authentication of those providers; and
- Providers are "touched" in order to become part of the HIE by a registration process and training.

Please refer to Exhibit A for a presentation that was made to the Clinical / Technical Committee on November 29, 2007, which provides an overview of the research completed.

As a result of determining the functional requirements for access to the HIE by the provider, the following standard definitions were adopted:

- Patient Health Summary - The ASTM / HL7 CCD standard is a patient health summary standard, a way to create flexible documents that contain the most

relevant and timely core health information about a patient, and to send these electronically from one care giver to another. It contains various sections -- such as patient demographics, insurance information, diagnosis and problem list, medications, allergies, care plan, etc. – that represent a "snapshot" of a patient's health data that can be useful, even lifesaving, if available when patients have their next clinical encounter. The ASTM / HL7 CCD standard is designed to permit easy creation by a physician using an electronic health record software program (EHR) at the end of an encounter.

- Policies / Procedures – Policies surrounding access to the HIE, participation agreements for using the HIE and how specific data elements will be used.
- Access – The process of obtaining data from, or placing into a computer system or storage device. It refers to such actions by any individual or entity that has the appropriate authorization for such actions. This term also applies to the policies and agreements shared between participating entities and the HIE.
- Authentication - Verification of the identity of a person or process. Authentication is also confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished using the presentation of an identity and credentials. To further define the authentication process in an electronic format, it is the process of establishing confidence in the user identifies electronically presented to an information system.
- Record Locator Service - An electronic health record locator that would help patients and their clinicians locate test results, medical history, and prescription data from a variety of sources. For example, physicians could use the locator to find out which other physicians have information on patients they are seeing. A record locator would act as a secure health information search tool and delivery system for health information.
- Master Provider Index – A software database program that collects provider information which serves as a core reference file access and authentication to the HIE. This can be accomplished using an active directory.

Progress of Legal Work:

The Legal Working Group (LWG) has made substantial progress in its three goals for Phase Two of the HISPC project. Specifically, we have developed: (1) proposed statutory and regulatory amendments that are necessary to remove barriers to e-health data exchange, and made progress toward development an enforcement and consumer rights framework for HIE in Arizona; (2) a draft model participation agreement to be used by HIEs in Arizona; and (3) draft model policies and procedures to be used by HIEs in Arizona.

Development of proposed statutory and regulatory amendments to support HIE: The LWG approached the statutory amendments in two phases. Phase 1 of the legislative work included developing proposed amendments to statutes regarding information regarding communicable disease, mental health, immunization, and genetic testing, and subpoenas for medical records. The meetings related to these statutory and regulatory amendments were held during the HISPC Phase One grant, but we received additional feedback from stakeholders during the HISPC Phase Two grant. At its September 2007 Board meeting, Arizona Health-e Connection Board of Directors decided to postpone the introduction of a legislative proposal for HIE until January 2009. This will allow Arizona Health-e Connection to develop a complete HIE "package" that establishes important consumer rights provisions and a more comprehensive enforcement framework, as well as remove the barriers to electronic exchange of health information within an appropriate privacy and security framework. Delaying the introduction of the legislation

will allow us to work with stakeholders and the Arizona legislature in advance, so that we can address potential concerns to the legislative package in advance of the session.

Phase 2 of the legislative work involves the ambitious project to create a new statute governing enforcement/ penalties for inappropriate access to an HIE, and potentially crafting immunity/ safe harbors for providers and other authorized individuals who access information in an HIE in an appropriate fashion. We facilitated a LWG meeting regarding these issues on November 13, 2007.

As exhibits to this report, we are attaching documents related to this work:

- Exhibit B. An August 17, 2007 memorandum from Coppersmith Gordon Schermer & Brockelman PLC to the LWG on the proposed statutory and regulatory amendments;
- Exhibit C. A September 17, 2007 Executive Summary of the proposed statutory and regulatory amendments;
- Exhibit D. An October 10, 2007 memorandum regarding revisions made to the proposed statutory and regulatory amendments;
- Exhibit E. The agenda for the November 13, 2007 meeting regarding an enforcement structure;
- Exhibit F. A chart of existing federal and Arizona statutes and regulations related to enforcement or safe harbors/immunity for providers; and
- Exhibit G. A summary of the November 13, 2007 LWG meeting.

Development of a model participation agreement and model policies and procedures to be used by HIEs in Arizona: The model participation agreement and model policies, when finalized, will establish model terms and conditions for provider access to HIEs in Arizona. To leverage work done across the country on HIE access agreements; we assembled existing resources for the participation agreements and policies, including the Markle Foundation and eHI Connecting Communities materials, to determine the best method for developing these resources.

We also formed a Best Practices Subgroup to research operational HIEs around the country to gather information on core policies and sample provider participation agreements. The issues of patient consent and consumer rights are critical to the success of the HIE effort. As a result, the research focused on these specific issues, while at the same time collecting basic information on other policy issues and agreement terms. (See research tool attached to October 9, 2007 memorandum. See Exhibit H & I) The Best Practices Subgroup interviewed the following existing HIEs about a variety of practices:

Long Beach Network for Health
Delaware Health Information Network
Indiana Health Information Exchange
Michiana Health Information Network
MA-SHARE
Lovelace Clinic Foundation
Taconic Health Information Network and Community (THINC)
HealthBridge
CareSpark
Volunteer eHealth Initiative
Utah Health Information Network (UHIN)
MedVirginia
Vermont Information Technology Leaders

Inland Northwest Health Services (INHS)

The Legal Working Group also held a series of meetings this fall to discuss in detail drafts of the model participation agreement and model policies and procedures for HIE, which took place on September 18, 2007, October 15, 2007 and November 13, 2007.

As exhibits to this report, we are attaching numerous documents discussed at these meetings:

- See Exhibit J. An August 17, 2007 memorandum from Coppersmith Gordon to the LWG regarding developing the model participation agreement and HIE policies and setting the September 18 meeting;
- See Exhibit K. The agenda for the September 18 meeting;
- See Exhibit L. A draft summary of the terms and conditions of an HIE agreement for discussion at the September 18 and October 15 meetings;
- See Exhibit M. A summary of the September 18 meeting;
- See Exhibit N. The agenda for the October 15 meeting;
- See Exhibit O. A draft summary of policy terms for discussion at the October 15 meeting;
- See Exhibit P. A summary of the October 15 meeting;
- See Exhibit Q. The agenda for the November 13 meeting;
- See Exhibit R. Draft HIE policies for discussion at the November 13, 2007 LWG meeting;
- See Exhibit S. Draft HIE participation agreement for discussion at the November 13, 2007 LWG meeting; and
- See Exhibit G. A summary of the November 13, 2007 LWG meeting.

Issues Encountered and Lessons Learned

During our work on this project, we encountered the following issues and gathered the following "lessons learned" from our research on a variety of technical options for provider authentication:

1) Public Key Infrastructure (PKI): PKI is a standard for strong authentication and can be deployed uniformly across multiple RHIOs. PKI enables "computer users without prior contact to be authenticated to each other, and to use the public key information in their public key certificates to encrypt messages to each other. In general, a PKI consists of client software, server software, hardware (e.g., smart cards), legal contracts and assurances, and operational procedures. A signer's public key certificate may also be used by a third-party to verify the digital signature of a message, which was made using the signer's private key. In general, a PKI enables the parties in a dialogue to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance, or even any prior contact." (See Wikipedia.org at http://en.wikipedia.org/wiki/Public_key_infrastructure.) It requires a Certificate Authority (CA) (such as Verisign) to handle certificate issuance. The benefit of PKI is that it enables parties to authenticate each other without exchanging secret information in advance.

   However, there are limitations to PKI. "The validity of a PKI between the communicating parties is, however, limited by practical problems such as uncertain certificate revocation, CA conditions for certificate issuance and reliance, variability of regulations and evidentiary laws by jurisdiction, and trust. These problems, which are significant for the initial contact, tend to be less

important as the communication progresses in time (including the use of other communication channels) and the parties have opportunities to develop trust on their identities and keys." (See Wikipedia.org)

2) Digital Signatures: "Digital signatures are used to create public key infrastructure (PKI) schemes in which a user's public key (whether for public-key encryption, digital signatures, or any other purpose) is tied to a user by a digital identity certificate issued by a certificate authority." (See http://en.wikipedia.org/wiki/Digital_signature.) A digital signature "is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or private key, and one for verifying signatures, which involves the user's public key. The output of the signature process is called the 'digital signature.' In other words, digital signatures can be used to authenticate the source of a message.

   The potential downside of digital signatures is that the user can only sign documents on a particular computer (unless the individual has a smart card that allows the use of the private key on any computer) and the security of the private key completely depends on the security of the computer, which is notoriously unreliable for many PCs and operating systems.

3) Biometrics: biometrics is a method "for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits," such as fingerprints, face recognition, hand geometry, iris recognition, keystroke dynamics or voice. (See http://en.wikipedia.org/wiki/Biometrics)

   The potential issue with the use of biometrics is that it can be slow and expensive to implement and use if there are large number of users. Biometric information is not able to be changed, therefore if it is compromised there is not an alternative for resetting.

4) Security Tokens: security tokens (i.e., smart cards, flash drives) are viable for RHIO deployment. These can be read like a credit card by inserting them into the PC. Combined with a user password they are effective for two-factor authentication.

   The distribution and expense of tokens may pose a barrier to using them in the HIE environment. Tokens can be easily misplaced, lost or stolen, as well.

5) Two-factor authentication: This method of authentication uses "something you know) (which could be a password), with "something you have" (a token, for example) or "something you are" (such as biometrics). For example a bank card is the physical something you have and the password (pin) to use that card is the something you know

   Some of the considerations in deploying two-factor authentications are:

   - If an organization is using many different applications, it is difficult to push the authentication package to the different applications
   - The users would need to remember two methods of logging into a system unless biometrics is used as one factor

- Interoperability across organizations becomes as issue as two-factor authentication is not standardized
- Increase in cost of authenticating

Each technical solution will need further research in order to determine the cost of the solution and the ease of implementation.

We also considered a variety of issues involved in the business processes around authentication.

1) "Local" registration and enrollment through participating entities: We determined that local registration and enrollment for users is viable for larger scale deployments to provide strong authentication, although establishing an enrollment strategy and process takes considerable time to formulate and implement. The biggest challenge is to ensure a smooth and manageable enrollment process for both the healthcare organization and the practitioner.

2) Policies and procedures need to be streamlined for the healthcare setting regarding the enrollment process using the Access Certificates for Electronic Services (ACES) program, which provides digital certificates and PKI services to enable electronic government applications. This is the program that was used by the HIMSS/GSA National e-Authentication Project and currently being piloted in several states.

3) During the HIMSS / GSA pilot, the participating states established a "local registration authority" (LRA) responsible for the initial registration of providers who would be accessing the HIE. Although a registration authority is an excellent idea, the process for completing the registration was extremely manual and cumbersome. The general steps were:

    a. Provider calls / emails RA authority to make an appointment;
    b. LRA goes to provider site;
    c. LRA has provider sign the participation agreement (agreement needs to be notarized and not all RA's were notarized);
    d. LRA must copy form at providers location;
    e. LRA loads authentication certificate software on the provider's PC; and
    f. Provider logins to computer and sets up user name and password

    In some cases, the LRAs were making two and three appointments with the providers to get them registered. Also, the certificate only works on the PC it is initially loaded on unless it is also on the provider's flash drive (if they have one).

    The process flow for authenticating and registering a provider will need to be more automated in order to be more efficient, even while using the ACES certificates for authentication. It was also found in one instance, the authenticating software was not compatible with the provider's computer infrastructure.

4) Each RHIO and HIE should perform a risk assessment to determine what is at risk if access is granted to the wrong individual or system. According to the HIMSS/GSA National e-Authentication Project Whitepaper, there are four levels of assurance used in addressing the risk factors. These are:

a. Level 1. Not assured that users are who they claim to be.
b. Level 2. Somewhat assured that users are who they claim to be.
c. Level 3. Very assured that users are who they claim to be.
d. Level 4. Absolutely assured that users are who they claim to be.

In performing the risk assessment, RHIOs and HIEs should also analyze what data is available to which provider or entity. For instance, there may be less risk in providing access to an office administrator for billing purposes than providing mental health treatment details to a general practitioner.

The HIMSS/GSA Whitepaper also recommends establishing "credential types" by using this combined method of analysis, which considers both assurance levels and data types. Appropriate credential types such as a username and password, digital signature, or token can then be selected depending on the levels of assurance and risk involved.

5) Much business variation exists within the area of user/entity verification methodologies. Credentialing services and pre-authentication by an outside trusted authority are a few of the practices currently employed to verify users.

6) There is also a lot of variation in business practices used to authorize access for providers who practice a multiple sites. This also means that there may be varying security levels for a provider. As stated in (4) above, this can be avoided if the proper method for analyzing the risk is employed.

7) Many entities have different passwords and logons for each IT application. This may pose a barrier to the implementation of an HIE sign-on unless we can achieve single sign-on capabilities as providers already have too many passwords to remember.

8) Methods for revoking access to the HIE need to be determined.

In addition, we have performed more detailed research regarding validation of the provider identity. We researched several other states' methods for obtaining this information and learned that many states are delegating the identity of providers. By using this method, the participating entity (i.e. hospital) would be required to download the participation agreement, sign and notarize. The form is then faxed to the HIE who is responsible for setting up the user ID and password for that entity. Once this process is completed, the participating entity provides the list of users that they are authorizing to access the HIE. We are hoping this user list can be transmitted electronically to the HIE. Each user is then set up and the authentication of that user happens when they access the HIE for the first time.

We also are challenged with developing a method to authenticate users who are not affiliated with the larger participating entities or who may not be licensed. We researched the potential use of the following information to support those efforts:

- NPI: We examined whether the National Provider Identifier database would support the authenticating of providers that are not affiliated with participating entities. Unfortunately, the NPI database will not support our efforts without additional information. The NPI was established to identify providers for payment purposes. A single provider can have more than one NPI depending on the type of provider and its Medicare billing practices. Most importantly, the company

that issues the NPI does not do any independent verification that the applying provider actually is a licensed health care provider.

- Health Profession Regulatory Boards: We also examined whether the local health profession regulatory boards, which issue licenses to physicians and other health care professionals, would have information valuable for HIE authentication purposes. We will need to discuss this issue with the health professional regulatory boards in much more detail. Even if we are able to arrange access to the boards' information, not every provider is licensed. For example, case managers, social workers, personal care attendants and various other health care professionals who may need to access the HIE are not required to be licensed. In addition, the health profession regulatory boards generally renew licenses every two years, and thus may not function as up-to-date information to authenticate providers.

Plans for continuing the project through the end of the year and, if applicable, after the end of the project:

The FTWG will meet through the end of December to continue research on the following open issues:

- Work with stakeholders to promote sharing of provider information by meeting with individual participant entities to discuss their methods of identifying and authenticating providers;
- Continue research on automating the participant authentication to the HIE and building the index of providers, and to review technical solutions for feasibility and cost of each for future reference;
- Continue planning for broad stakeholder outreach and education;
- Continue researching other HIEs to determine other methods for authenticating providers who are not associated with a participating entity; and
- Research single sign-on methods to determine feasibility.

The Legal Working Group will continue to work on the model participation agreement and policies for HIE, as well as continue to refine the proposal of statutory and regulatory amendments, including a statutory enforcement framework for inappropriate access to the HIE. We do not have further in-person meetings of the LWG scheduled, but will continue to make revisions to these documents, for which we will seek feedback from the LWG via email or teleconferences.

In addition, we plan to do additional follow-up with stakeholders outside of the LWG participants, including: (1) discussions with in-house legal counsel of Arizona hospitals (through the auspices of the Arizona Hospital and Healthcare Association); (2) discussion with legal counsel for the Arizona Medical Association; and (3) broad circulation of the drafts to the Arizona Health-e Connection Board of Directors and its newly formed Consumer Advisory Council.

Both the functional/technical and the legal work will continue in 2008, as supported by available funding and the strategic planning of Arizona Health-e Connection.

Impact Analysis-- Major Milestones of the Arizona Health Privacy Project

Both the functional and legal work in HISPC Phase Two continued to involved a large number of stakeholder in the planning and development of HIE capacity in Arizona. The work has identified the need for continued work in a number of areas.

Functional:

The AHPP functional team conducted several individual meetings with major stakeholders to communicate the proposed process requirements that we have outlined and to discuss their methods of authenticating providers and assigning access to private networks and electronic medical records systems. In addition, the project progress was reported to the Executive Committee of AzHEC on a monthly basis and to the Clinical / Technical Committee of AzHeC monthly.

As a result of these meetings, we identified the need for continued work in the following areas:

- Develop a method in the community to achieve single sign-on for providers. This is a challenge because many applications may be in use at different participating entities, requiring several different logins and passwords (even within one institution).
- If an HIE expects to obtain a list of authorized users from the participating entities, we should develop an electronic method for adding this information to the HIE directory of providers. Automating this process might be costly and add extra burden on IT departments.
- Work closely with our hospitals, community health centers and other health care organizations to develop the trust necessary for these providers to allow the HIE to obtain a list of authorized users electronically.
- Conduct future research on the cost of using tokens, biometrics and digital signatures to authenticate users, as well as PKI.
- Work on how to authenticate providers who are not affiliated with participating entities (such as physicians who do not have medical staff privileges at a hospital).
- If an HIE wants to provide access to individuals that are not licensed health care providers, we will have an additional challenge in authenticating those individuals if they are not affiliated with a participating entity.

Overall, the consensus has been that we need to make the HIE registration process easy for providers and we need to leverage existing organizations that are credentialing, identifying and authenticating providers. Additionally, the methods we use will need to be communicated to consumers as well in order to build a comfort level in the community with sharing electronic health information.

It is apparent that the technology can be applied to access and authentication depending on cost however the process for obtaining the information accurately and timely will be more challenging. By using the appropriate communication and partnering with the participating entities we are hopeful this can be accomplished.

Legal:

We have accomplished a great deal of legal work related to the development of HIEs in Arizona. This includes a comprehensive package of proposed statutory and regulatory amendments, a model participation agreement, and a model set of policies and procedures for HIEs developing in Arizona. We have involved a wide range of

stakeholders in the legal work and so we expect the Legal Working Group analyses and materials to achieve wide acceptance in the community.

In 2008, we will need to engage in outreach and education to consumers, providers and the Arizona legislature to raise awareness of HIE and the need for the proposed statutory and regulatory amendments through the Arizona. If the legislative package is introduced in January 2009, there will be a substantial amount of work that will occur in the last quarter of 2008, through the first half of 2009, to shepherd the proposed statutory amendments through the Arizona legislature.

Also in 2008, we will need to revist the model participation agreement and model policies and procedures for HIE, as the HIEs develop concrete plans for the architecture of the HIEs. This will need to be an evolving set of documents to be responsive to the needs of Arizona HIEs.

We also have the challenge of doing wider outreach to consumers. This will be made possible by the new development of the Arizona Health-e Connection Consumer Advisory Council. Utilizing feedback from consumers and a wide array of providers, we need to resolve important policy decision on HIE, particularly whether and how consumer consent will be sought to include information in the HIE.

Future Vision

Are there any specific challenges to private and secure interoperable HIE identified in Phase One that still need resolution?

The barriers identified in HISPC Phase One included:

- Variations in communication media
- Variations in interpretation of HIPAA
- Variations in security procedures – authentication & authorization
- Organizational size and financial constraints
- State law barriers
- Information exchange issues between state, Indian Health Service and the sovereign Native American Nations

The solutions identified to address these barriers were:

- Developing a regional health information exchange
- Solutions for authorization and authentication problems
- Solutions for secure information transmission or exchange
- Solutions to prevent unauthorized modifications
- Solutions for current paper-based systems, primarily focused on information exchange by fax
- Enhancing patient's role in controlling their personal health information
- Other solutions
- Solutions affecting state law/regulations
- Solutions affecting federal law/regulations

Although the AHPP Team has been able to address access and authentication for providers access to the HIE, we still have many other security and privacy issues that will need to be resolved. The following solutions will be partially addressed by this project for provider access to the HIE:

- Solutions for authorization and authentication problems
- Solutions for secure information transmission or exchange
- Solutions to prevent unauthorized modifications
- Solutions affecting state law/regulations

What is the plan and/or commitment within the state to resolve these issues?

We will be producing a high level list of action items and a budget to present to the Arizona Health-e Connection Board of Directors. We hope that the project will be funded so we can continue working through the privacy and security issues in state, in addition to the work we will do as part of the Standards Collaborative.

What interactions between states that have been of value?

Arizona attended the collaborative meetings in Chicago, Denver and Washington DC as part of the HISPC project collaborative work that is being proposed to the ONC. These meetings were enlightening to learn about other business models and the challenges encountered in other states. We have also found most states seem to be following the same general path as they address security and privacy issues. This should allow for ease of implementation when we address inoperability among states.

These meetings also were very valuable in helping assess the methods for access and authentication for providers to access the HIE. Arizona will be working with Connecticut, Colorado, Utah, Washington, Virginia, Maryland, Oklahoma, Nebraska and Ohio on a collaboration to address standards adoption around access, audit and authentication, in order to facilitate inoperability between states sharing health information electronically.

What are intended outcomes of the collaborative work?

This collaborative will explore differences in the concept, design and business models for HIE in various states and their implications for health care privacy and security practices. Once these are articulated, the group will seek to define HIPAA-compliant business practices and standards by which these HIE may share information with authorized and authenticated providers in other states. These business practices will address the minimal audit standards and procedures to assure appropriate identification, including access control and authentication when conducting interstate HIE.

The collaborative will focus on two related objectives that should assist with our stated purpose: 1) development of policy requirements; and 2) definition of an implementation strategy. Through these two outputs, the collaborative will develop sufficient descriptive background material to permit any state to begin design or understand proposed requirements for interstate HIE.

Within the objectives stated above, the specific scope of the project is to focus on developing background material (policy requirements and implementation strategy) for three unique privacy and security domains:

- o Audit: a clearly defined set of audit requirements, associated data elements, and the processes by which an HIE monitors the exchange of information across state lines. These data and processes would provide a mechanism to assess the appropriateness of exchange were there to be a need for more in-depth review;

- o Provider identification (including authentication and access controls): establish the minimum requirements for authentication within an HIE that will permit sufficient interstate trust to exchange information. Minimum standards, including processes for establishing identity service providers, transmitted data elements, data exchange format, and conformance measures are needed for role-based, interstate HIE access;
- o Patient identification: a definition of the minimum standards (including data elements and format), processes and requirements needed to search for a patient, the acceptable level and extent of exposure of patient information to the provider doing a search, and what parameters will be used to limit that exposure.

While policies and an implementation strategy may be developed and shared during the project period, until physically implemented across two states (where data sharing is probable or exists), we are uncertain of their generalizability and cross-state utility. The collaborative intent is to broadly study all three policy areas during this period; however, we may have partial capacity to comprehensively evaluate all policy components during the project period. Finding the ideal environment (where there is effective exchange within two states) and the need for interstate exchange between those states may be limited. Thoroughly addressing all three of the policy areas during this project period may be incomplete, but the collaborative has set that as our collective goal.

Conclusion

Our findings from the Functional / Technical Working Group have reinforced that, although there is viable technology (PKI, digital signatures, tokens) that can be used to authenticate providers to access an HIE, the business practices and workflow will be a challenge.

We recognize that further research is required to develop efficient, yet rigorous, methods to identify providers, to authenticate users who are not licensed health care professionals, and to authenticate users or who are not affiliated with or employed by an entity participate in an HIE. We anticipate recommending to the Arizona Health-e Connection Board of Directors the use of the HIMSS/GSA e-Authentication Whitepaper as the standard document for analyzing authentication needs, as well as using the ASTM standard combined with HL7 for a continuity of care record.

Our Legal Working Group has made substantial progress in developing proposed legislative and regulatory amendments to remove barriers to HIE in Arizona and to create a rigorous enforcement environment for HIE. It also has developed a model participation agreement and model policies and procedures for HIE in Arizona, which will assist in providing “policy interoperability” between HIEs developing in Arizona.

Both the Functional/Technical Working Group and the Legal Work Group recognize the need for continued stakeholder outreach, including to consumers.

Our future work on privacy and security will be enhanced by the multi-state Standards Collaborative, which is due to commence in January 2008. The collaborative will analyze models of HIE and various methods for auditing, allowing access and authenticating providers, which will allow Arizona to continue the work we have started in this phase of the HISPC project.

Exhibit A

Technical/Clinical Subcommittee meeting

Mary Kay McDaniel

Kim Harris-Salamone, Ph.D.

Agenda

- Review Scope of Work
- Types of HIEs
- Review of Functioning US HIEs
- Review of Standards
- Barriers
- Recommended next steps

Original Scope of Work

- Identify standards used by functioning HIEs
- Identify lessons learned
- Identify committee next steps

Actual Scope of Work

Through a string of emails the scope became:

- Review other states that have HIEs and identify standards
- Review each large hospital in Phoenix and the standards they are using
- Compare standards used in Phoenix to other HIEs
- Review national standards for consistency
- Supply recommendations for Arizona to use
- Identify first projects, core technical and data standards

Interview questions

- What was the start-up project or application?
  - Are these projects/applications in test or production?
  - What types of facilities were the initial major players?
  - What types of data were exchanged?
- Has it expanded from there?
- With regard to the Core Technical standards, please identify the standards used for:
  - Network connectivity (i.e., Internet Engineering Task Force (IETF) Transmission Control Protocol/ Internet Protocol (TCP/IP) Version 4)
  - Web applications (i.e., http, https)
  - Transport encryption (i.e., IETF Transport Layer Security (TLS) Version 1.0/Secure Socket Layer (SSL) Version 3.0)
  - Authentication (Username/Strong Password Public Key Infrastructure (PKI) Hardware Tokens, Biometric Devices)

Interview questions

- With regard for the HIT infrastructure and applications, please identify which standards your exchange utilizes for:
  - Application architecture (i.e., Multi-tier, with separation between presentation layer, business logic, and data Service-Oriented Architecture)
  - Clinical Context Management (CCOW)
  - Database access standards (SQL, etc.)
  - Directory Services (Active X, LDAP)
- Do you have Single Sign On (SSO) capabilities? If so, please describe the authentication process.
- Is there a set of standard terminologies used for process interoperability? (Is everyone required to use them?) Such as:
  - ICD9
  - CLIA
  - LOINC
  - SNOMED CT
  - CPT4
  - DICOM
  - NDC

Interview questions

- Does an EHR have to be CCHIT certified in order to connect to the HIE?
- Where does the transformation occur in the exchange when messages come in and go out of a participant's system?
  - Is there a specific software package that does the transformation and how do they validate conformance of messages? Or
  - Does the participant write their own and how do they validate conformance of messages?
- Do you have a centralized provider index?
  - If so, how do maintain this?
  - How do you authenticate providers and where are you getting the provider information from?

Interview questions

- Do you have a centralized patient index?
  - If so, how do you maintain this?
  - How do you authenticate patients and where are you getting the patient information from?
- What messages/transactions are you currently exchanging? [please include Standard and Version.]

Bumps in the Road

- No clear, agreed upon standard definition for Health Information Exchange
- Follow-up on recommended HIEs suggested identified HIEs in planning stages, initial implementation imminent, dates moved back. Very few actually exchanging data [as in two way communication]
- Lack of understanding of what AzHeC will initially support/ encourage. No problem statements or use cases developed.

Standard

- something considered by an authority or by general consent as a basis of comparison; an approved model
- an object that is regarded as the usual or most common size or form of its kind
- a rule or principle that is used as a basis for judgment

…dictionary.com

Standardization

- The term **standardisation** or **standardization** can have several meanings depending on its context. Common use of the word standard implies that it is a universally agreed-upon set of guidelines for interoperability. However, the plurality of standards-issuing organizations means that a document purporting to be a "standard" doesn't necessarily have the support of many parties.
- As Grace Hopper said, "The wonderful thing about standards is that there are so many of them to choose from".
- In the context of technologies and industries, standardization is the process of establishing a technical specification, called a standard, among competing entities in a market, where this will bring benefits without hurting competition.

    - www.wikipedia.com

Types of Standards

- Screen Design – what does it look like
- Programming Language – what is it written in
- Communication Protocols – how does it get there
- Security – who are you, do you have permission
- Interface – what do you want
- Vocabulary – are we talking about the same thing

Types of Standards

St. Lucia Bureau of Standards says:

A standard is a precise and authoritative statement of the criteria necessary to ensure that a material, product or procedure is fit for the purpose for which it is intended. These fall into six categories namely:

- Glossaries or definitions of terminology
- Dimensional standards
- Performance Standards
- Standards Methods of tests
- Codes of Practise
- Measurement Standards

Types of Standards

- ***de facto***
  - one that is based on widespread use and recognition throughout an industry
- ***de jure***
  - standard that is created by a body or committee
  - These two types of standards are not mutually exclusive, and often, the best standards are those that start as de facto standards then become de jure standards. This is because unproven de jure standards are less likely to be successful.

Types of HIE

- **Clinical messaging** – delivering of clinical results on a push basis
- **Administrative** – movement of HIPAA mandated transactions between providers and payers
- **ePrescribing** – movement of prescription-related transactions among providers, PBMs and pharmacies
- **Patient Summary** – the ability to retrieve a comprehensive set of clinical data from regional providers
- **Quality Measurement** – not yet attainable
- **Biosurveillance or syndromic surveillance** – involving the monitoring of clinical data for disease outbreak or bioterrorism event
- **Chronic disease management** or other population-based services

Functioning US HIEs

- Challenging to identify
  - Given recommendations to start to contact
  - Knew of some
  - Reviewed literature
  - Few actually exchanging data
- Generally one way [PUSH]
- Clinical messaging has been more readily adopted [lab results, medication history]

Findings

- There are a lot of state's and organizations talking about HIE
- There are a lot of conferences discussing and reviewing HIE
- There are a lot of $s being spent/promised on/to HIE
- There are a lot of ways to do HIE

Findings

Development of State Level Health Information Exchange Initiatives

Final Report: Extension Tasks

January 23, 2007

Contract Number: HHSP23320064105EC

Foundation of Research and Education of American Health Information Management Association

[The information on the following slides was taken from TASK #2, “Report and Recommendations on Health Information Exchange Services That are Financially Sustainable”]

Clinical Messaging

- HealthBridge (source: FORE report and Interview)
  - Standards: HL7, LOINC, EMR feeds are standardized across the region
  - Data Sources: Hospitals (21) and labs (2)
  - Exchanging lab, admission, and discharge data only
  - Axolotl's HIE edge servers (based on HL7, but built own IG)
- Regenstrief Institute/Indiana Health Information Exchange (source: FORE)
  - Standards: HL7, LOINC
  - Data Sources: Hospitals (16) and labs (2)
  - Centralized data repository (DOCS4DOCS)
- Inland Northwest Services (source: FORE and Interview)
  - Standards: HL7, Partial LOINC
  - Data Sources: Hospitals (34), labs (2) and regional imaging center (1)
  - Meditech software used by [all] participants – centralized servers
  - 3 EMR feeds (Centricity, NextGen, and Practice Partners)
  - Offer Centricity's ASP EMR/PMS to participants

Patient Health Summary

- Regenstrief Institute/Indiana (source: FORE report)
  - Standards: HL7 formatted messages; all laboratory results are mapped to LOINC by Regenstrief.
  - Data Sources:
    - 20 hospitals
    - Indiana State Department of Health
    - Marion County Health Department
    - RxHub (PBM consortium)
    - Regional reference laboratories
    - Radiology centers
    - Multiple physician practices
    - Medicaid claims data (new and will go live –need f/u)
    - Commercial payer claims data (several contracts have been signed and data has been received and is being evaluated for incorporation)
    - Medicare (has committed to providing some data for limited purposes under a grant)
  - Note: access is severely limited to credentialed physicians at a specific facility (approximately 3K physicians)

Medication History

- Regenstrief Institute/Indiana (source: FORE report)
  - Standards: HL7
  - Types of data: Medication history, formulary

E-Prescribing

- Regenstrief Institute/Indiana (source: FORE report)
  - Standards: HL7; NCPDP message formats; NDC, Medispan CPI, and RxNORM CUI codes
  - Types of data: Medication history, formulary

Administrative Data

- UHIN (Utah Health Information Network) (source: FORE report)
  - Standards: HIPAA X12 format
  - No centralized data repository
- NEHEN (New England Healthcare EDI Network) (source: FORE report)
  - Standards: ANSI HIPAA format (X12)

Security Standard For Authentication

- These health informatics standards specify requirements for use of PKI, directory services and authorization privileges in healthcare:
  - ISO IS17090: Health informatics: PKI (Parts 1/2/3) (supersedes ISO TS17090 Health Informatics—PKI (Parts 1/2/3).
  - ISO TS21091: Health informatics: Directory services for security, communications and identification of professionals and patients.
  - ISO TS26000: Health informatics: Privilege management infrastructure (Parts 1/2/3).
  - ISO ISO DTS21298: Health informatics: Functional and Structural Roles.
  - ASTM E1986: Standard Guide for Information Access Privileges to Health Information.
  - ASTM E1762: Standard Guide for Electronic Authentication of Health Care Information.
  - ASTM E2084: Standard Specification for Authentication of Healthcare Information Using Digital Signatures.
  - ASTM E2212-02a: Standard Practice for Healthcare Certificate Policy.
  - IHE Audit Trail and Node Authentication Profile (ATNA).
  - IHE Document Digital Signature (DSG).
  - IHE Cross-Enterprise User Authentication (XUA).

HIE/RHIO Authentication: HIMSS/GSA

- National e-Authentication Project
- Pilot that tested the GSA's e-Authentication Service Component program to provide digital certificates, technical architecture development support and certificate validation services.
  - Incorporates 2 different architectures: assertion-based authentication and certificate-based authentication
  - Users authenticate to a Credential Service Provider (CPS), who asserts their identity to the Agency Application – digital certificates in a PKI (standard: ISO TS17090)
- The ACES (Access Certificates for Electronic Services) program
- Manual registration process to establish authentication for digital certificates
- No one actually exchanging data yet (6/07)

Pilot Results: Connecticut

- CT – CT RHIO communities in Middlesex, Hartford, and Bridgeport areas (part of HISPC)
  - Unable to initiate the revised IS17090 Health Informatics – PKI International Standard due to the lack of configured support in the CA supporting the test environment
  - Used ASTM E1986 to configure the portal environment – have SSO in 2 of the provider portals based on the ACES certificates
  - Dept of Public Health is the issuing authority of medical credentials
  - Local registrar used face-to-face registration to issue hardware-based identities and encryption certificates in accordance with the ACES vendor's CPS. Modified process, similar to QNET
  - Not yet operational at time of whitepaper (6/07)

Pilot Results: Southeast Michigan

- MiHIN statewide RHIO – Data Sharing & Transaction Infrastructure Project
- Pilot to focus on secure interchange of healthcare data across disparate stakeholders to evaluate the feasibility of using e-Authentication in healthcare.
- Organized the vetting process for the credentials to begin with a physical visitation with the designated LRA
- Difficulties and concerns – logistics, LRAs did not specify that documents could not be faxed or copied, but had to be replaced with mailed, signed originals.
- Tests showed some issues but that the underlying technology does work – Groupwise 6.5 has still posed unresolved issues in processing certificates
- Not live as of the whitepaper (6/07)

Pilot Results: Minnesota – Community Health Information Collaborative

- Project was to develop a SSO service, using the ACES certificates – proof of concept that federated identity management and digital certificates could be a viable solution to the SSO objective.
- Results: Registration of certificates process involved 2 phases – test between the project's 2 co-leads who were identified and trained as LRAs. One of the co-leads was successful in completing the registration process, on-line, and ultimately received certificate and reached the test servers. Other co-lead was unable to receive certificate.
- Support structure, when problems arose, was hard to reach and resolution was slow.
- Once the ACES certificates were received (by 3 physicians), installing and using them was a matter of adding them to the access control lists on the 2 hospital systems.
- Due to existing Minnesota privacy laws, the test did not exchange data. It was designed to test a proof of concept. Both hospital systems set up test servers – to be replaced with the hospitals' test Citrix systems.

Pilot Results: Ohio – Supercomputer Bioinformatics

- Research focused
- Clarified logistics and procedures required for establishing individual authentication at local and remote collaborating research sites
- Issues identified:
  - Staff turnover was an issue
  - Face-to-face between LRA and individuals issue – especially for remote users (logistics)
  - Accurate and complete documentation
  - Lack of on-site notary public

Pilot Results: Ohio – Virtual Medical Network (VMN)

- VMN is a turnkey enterprise solution for PMS, EHR, Billing, Scheduling, E-prescribing and transcription
- Problem when exporting data out of network
- Manual registration process for two physicians (in/out network)
- Incompatibility issues: VMN operated on Internet Interoperability Standards (IIS)5 and needed to be moved to an IIS6 in order to work.
- Certificates are resident files on a specific piece of equipment or hardware-based device. In order for an authenticating server to process the certificate, the request must either be made from the same physical piece of equipment or the physician must carry the certificate file in some portable manner AND be compatible with all types of PCs or laptops that might be used for the access request.

Pilot Results: Texas – Corpus Christi

- Purpose – to improve emergency treatment by first responders
- 3 people were identified who were willing to act as LRAs – 1 completed the registration process. The actual registrations have yet to occur.
- FBI had installed software for paramedics to use – FBI protocol prohibits the addition of any other applications to the server.
- Data exchange has yet to occur

Pilot conclusions

- PKI, as a standard for strong authentication, can be deployed uniformly across multiple RHIOs
- Enrollment is the most difficult part of deployment
- Policies and procedures need to be streamlined regarding the enrollment process using the ACES certificates
- Each RHIO must identify a risk assessment process for the sensitivity of the data being exchanged

Web review of HIEs

- Organizations Exchanging Data
  - 7
- Limited/specific exchanges
  - 8
- Unclear if any exchanges are actually occurring
  - 5
- Planning/beginning implementation stages
  - 7

Which ones do we care about?

- Depends on the ‘type’
  - Terminology versus transport versus interface
- Examples
  - Marital Status
  - NDC

Wikepedia	2000 Census	834
Married	Now Married	Married
Single		Single
Separated	Separated	Separated
Divorced	Divorced	Divorced
Widowed	Widowed	Widowed
Engaged		
Annulled		
Cohabitating		
Deceased		
	Never Married	
		Registered Domestic Partner
		Unreported
		Unknown
		Legally Separated

NDC (National Drug Codes)

- NDC codes = product ID codes
- Unique product IDs used by pharmacies, PBMs, and payers
- Code structure
  - Manufacturer | Product | Package
  - ‘Manufacturer’ assigned by FDA
  - ‘Product’ & ‘Package’ assigned by manufacturer
  - Not standardized within or across manufacturers

Code	Meaning
00686-0201-02	Acme | Furosemide 10 mg tablets | 200 count bottle
00686-0202-15	Acme | Furosemide 20 mg tablets | 200 count bottle
05831-4065-30	GenRx | Furosemide 20 mg tablets | 200 count bottle

NDC codes continued

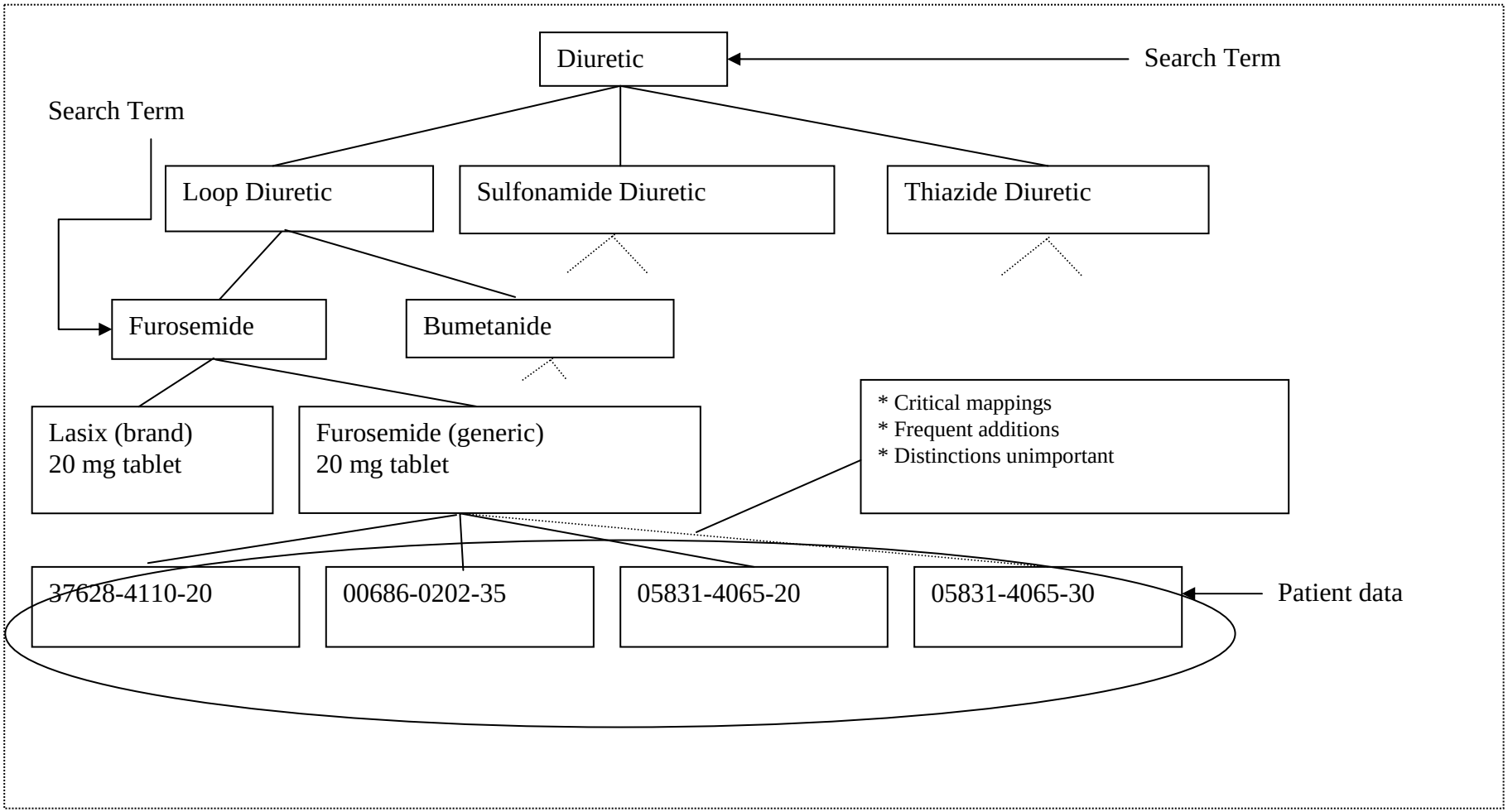
- Representation
  - 12, 11, or 10 digit codes (11 most common)
  - Hyphenated or non-hyphenated components
  - If 10 digits and non-hyphenated, you have to know the pattern
- Examples (all same drug)

# digits	Pattern	Hyphenated	Non-hyphenated
12	6-4-2	000686-0244-02	000686024402
11	5-4-2	00686-0244-02	00686024402
10	4-4-2	0686-0244-02	0686024402
10	5-4-1	00686-0244-2	0068602442
10	5-3-2	00686-244-02	0068624402

NDC Codes continued

- Most widely used coding standard for medications
- Distinctions often not clinically relevant
  - “Acme | Furosemide 20 mg tablets |100 ct bottle”
  - “Acme | Furosemide 20 mg tablets | 200 ct bottle”
  - “GenRx | Furosemide 20 mg tablets | 200 ct bottle”
- Mapping to clinical concepts is needed for most EHR functionalities

NDC codes continued



Next Steps

- Decide on the Model for the Exchange
- Narrow the Scope
  - Identify first project, core technical and data standards
  - Decide what data elements to exchange, et. al…
  - Develop work plan
  - Develop our own IG based on standard/version chosen for identified messages
- Review with willing trading partners for the initial projects

Exhibit B

Coppersmith Gordon Schermer & Brockelman PLC

MEMORANDUM

DATE: August 17, 2007

TO: Arizona Health-e Connection Legal Working Group

FROM: Kristen B. Rosati

RE: Arizona Health Privacy Project Phase II –
Finalizing Proposals for Statutory and Regulatory Amendments

This fall, the Legal Working Group of the Arizona Health Privacy Project will continue its work on proposals for legislative and regulatory changes where we have identified laws that pose barriers to the implementation of e-health information exchange (HIE).

As you may know, we are approaching the statutory amendments in two phases. **Phase 1** of the legislative project includes proposed amendments to statutes regarding information regarding communicable disease, mental health, immunization, and genetic testing, and subpoenas for medical records. Based on our productive June 12 meeting and further work with the subcommittee chairs, this memorandum outlines a draft proposal for those statutory changes. **Please provide any feedback by August 30.** I will then will refine the proposals and present them to the Arizona Health-e Connection Board of Directors for approval on September 18, 2007.

Phase 2 of the project involves the ambitious project to create a new statute governing enforcement/ penalties for inappropriate access to an HIE, and potentially crafting immunity/ safe harbors for providers and other authorized individuals who access information in an HIE in an appropriate fashion. The first meeting to discuss an enforcement proposal will be **October 15, 2007, 9 a.m. to 12 p.m.** at 1700 West Washington Street, the Tower's First Floor Conference Room. Please RSVP to Kim Snyder before September 16 at ksnyder@azgita.gov or voice mail at 602-364-4795. The chairs of the enforcement subgroup have been hard at work and I will circulate proposals in advance of the meeting for your review.

Beth Schermer and I sent out a second memorandum today regarding the development of model policies and a model participation agreement for HIE, which is also part of the second phase of activity under the Health Information Security and Privacy Collaboration grant. We hope that you will be interested in getting involved in that project, as well.

Thanks, as always, for your involvement!

1. Background

As you know, we created the following subgroups to evaluate and outline potential statutory or regulatory amendments to remove barriers to e-health data exchange:

- Communicable disease information statutes and regulations: A.R.S. § 36-661 *et seq*., A.R.S. § 20-448.01 and A.A.C. R20-6-1204 (Chair: Laura Carpenter, The Carpenter Law Firm)

- Mental health information statute: A.R.S. § 36-501, *et seq*. (Chair: Bob Sorce: Arizona Attorney General's Office, representing Arizona Department of Health Services Behavioral Health Services Division)

- Immunization information: A.R.S. § 36-135 and A.A.C. R9-6-708. (Chair: Elizabeth Dietz, Arizona Attorney General's Office, representing Arizona Department of Health Services)

- Genetic testing statutes, A.R.S. § 12-2801, *et seq*. and A.R.S. § 20-448.02, *et seq*. (Chair: Ira Berkowitz, St. Joseph's Medical Center)

- Medical record subpoena statute, A.R.S. § 12-2294.01 (Chairs: Bonnie Peterson, HIM Department Chair, Phoenix College; and Brigid Holland, Director Health Information Management, Navapache Regional Medical Center)

- AHCCCS member information regulations: A.A.C. R9-22-512 (Chair: Matt Devlin, Assistant Director, Office of Administrative Legal Services, AHCCCS)

- Adult Day Health Care Facility records regulation: A.A.C. R9-10-511(C) (Chair: Open)

- Enforcement (Chairs: Barbara Hess, Senior Financial Analyst, Pinal/Gila County Long Term Care and Timothy Miller, Executive Director, Arizona Medical Board; other members include Denise Holtcamp, Medical Investigative Nurse, CRM/SIS, Office of the Attorney General)

- Immunity from enforcement or civil liability (safe harbors) (Chair: Ira Berkowitz, St. Joseph's Medical Center)

This memorandum provides background for individuals who have not been able to attend all of the meetings: it describes the laws related to sharing of the types of information identified above and the barriers we have identified in these areas.

This memorandum also describes the consensus position we developed at the Legal Working Group meeting on June 12 regarding how to approach amendments to the communicable disease, mental health and immunization statutes. It also describes a

proposal for amending the medical record subpoena statute and the genetic testing statutes, which we did not have a chance to discuss in detail in June. Finally, the memo describes the statutory and regulatory amendments the Legal Working Group could propose to the Arizona Health-e Connection Board at its September 18 meeting. Your consideration of these proposals and feedback is welcome.

If the Arizona Health-e Connection Board approves our recommendations for statutory revisions, we will begin the process of engaging stakeholders across the state to ensure that our recommendations reflect a broad consensus and accommodate diverse interests. We anticipate that a bill will be introduced at the beginning of the next legislative session in January.

Finally, we will be working with AHCCCS, ADHS and DOI regarding proposed amendments to the regulations we identified as potential barriers to HIE, to arrive at a consensus with the agencies. Because each agency is on a different schedule for reopening the agency's regulations, it may take a number of years to accomplish all regulatory change.

This is an open process, so please feel free to forward to individuals you think would be interested in these topics. Your feedback is appreciated, as always!

2. Proposed Statutory Amendments for Consideration by the Arizona Health-e Connection Board of Directors

The following section provides details regarding the present laws, how those laws may constitute barriers to HIE, proposed statutory amendments, and our reasoning behind these proposals.

(1) Communicable Diseases:

A.R.S. § 36-661 *et seq.*, A.R.S. § 20-448.01 and A.A.C. R20-6-1204

Description of Laws:

Arizona law requires certain health care providers and administrators of health care entities to report to the local health agency and others when they identify a case or suspected case of certain communicable diseases. In the case of HIV, AIDS, and tuberculosis, the specific reporting requirements are identified in statute.[1] In addition to these specific statutory requirements, ADHS regulations identify additional reportable communicable diseases.[2]

Healthcare providers must preserve the confidentiality of reportable communicable disease information and may release it only for the purposes expressly listed in the

[1] A.R.S. § 36-621 (HIV/AIDS), A.R.S. § 36-723(D) (tuberculosis).

[2] A.A.C. R9-6-101 et seq.

statute.[3] Communicable disease information is broadly defined information and goes far beyond HIV/ AIDS information; it includes information about any "contagious, epidemic or infectious disease required to be reported to the local board of health" or ADHS that is in the possession of someone who provides health services or who obtains the information pursuant to a release (same as a "consent" or "authorization") signed by the patient.[4] At present, reportable communicable diseases include a wide variety of ailments, including flu, measles, mumps and other conditions that do not carry a stigmatizing effect.[5] Separate provisions govern when a state, county or local health department or officer may disclose communicable disease related information.[6] Given the broad scope of "communicable disease information," a HIE will certainly include communicable disease information.

Significantly, if a disclosure of communicable disease information is made for a purpose for which an authorization is required, the disclosure must be accompanied by a statement "in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law."[7] Where the information is disclosed to a person pursuant to a patient's authorization, the person receiving the information also must comply with the statute.[8]

Finally, additional restrictions in the Insurance Code apply to health plans' release of HIV/AIDS information. The insurance statute lists limited types of disclosures of HIV/AIDS information that insurers are permitted to make. [9] Like health care

---

[3] A.R.S. § 36-664.

[4] A.R.S. § 36-661(4) and (5).

[5] See R9-6-202 (Reporting Requirements for a Health Care Provider or an Administrator of a Health Care Institution or Correctional Facility; R9-6-203 (Reporting Requirements for an Administrator of a School, Child Care Establishment, or Shelter); R9-6-204 (Clinical Laboratory Director Reporting Requirements); R9-6-205 (Reporting Requirements for a Pharmacist or Pharmacy Administrator); R9-6-206 (Local Health Agency Responsibilities Regarding Communicable Disease Reports); R9-6-207 (Federal or Tribal Entity Reporting).

[6] A.R.S. § 36-661. These persons may disclose this information only if:

(1) Specifically authorized or required by federal or state law;
(2) Made pursuant to an authorization signed by the protected person or the protected person's health care decision maker;
(3) Made to a contact of the protected person (someone who may have contracted the disease). The disclosure shall be made without identifying the protected person;
(4) For the purposes of research as authorized by state and federal law;
(5) With authorization from the director, to the national center for health statistics of the United States public health service for the purposes of conducting a search of the national death index.

[7] A.R.S. § 36-664(H).

[8] A.R.S. § 36-664(A).

[9] A.R.S. § 20-448.01.

providers, an insurer's disclosure of HIV/AIDS-related information must be accompanied by a written statement that warns that the information is protected by state law that prohibits further disclosure of the information without the specific written consent of the person to whom it pertains or as otherwise permitted by law.[10]

Moreover, when insurers seek authorization from individuals to release HIV/AIDS information, A.A.C. R20-6-1204 places additional restrictions on those disclosures and imposes an 180-day limit on an authorization form.

Identified Barriers to Health Information Exchange:

A.R.S. § 36-664(H) and A.R.S. § 20-448.01(G) require that communicable disease or HIV/AIDS information disclosed pursuant to an authorization be accompanied by a written statement that warns the information is confidential and prohibits further disclosure without the specific written authorization of the patient or as otherwise permitted by law. This requirement for a written statement regarding re-disclosure may pose a substantial barrier to HIE. Because the definition of "communicable disease" is so broad and includes many health conditions such as flu (see discussion above), health care providers cannot segregate communicable disease information from the rest of the information in a patient's record. We thus must assume that all health information exchanged in a HIE includes communicable disease information. This will pose a barrier to HIE in the following circumstances: if an individual provides authorization to include his or her health information in the HIE (either collected by the provider or the HIE), information about that individual would need to be accompanied by a written re-disclosure warning when it was disclosed to the HIE and every time that information was disclosed by the HIE. The requirement that such notice be "written" poses obvious challenges in the electronic health information environment. But even if an electronic notice meets the written notice requirement, existing electronic health information systems cannot accommodate such a requirement.

Moreover, both A.R.S. § 36-664 and A.R.S. § 20-448.01 could be interpreted as not permitting direct disclosure of information to an HIE. Both statutes expressly list permitted disclosures, which do not include an HIE. Moreover, the insurance statute does not even permit disclosures for treatment purposes without the consent of the patient.

A.A.C. R20-6-1204 also limits an insurer's ability to release information to an HIE, as it requires a written release form for any disclosure of HIV-related information. Moreover, the 180-day limit on an authorization form would limit the ability of an HIE to handle this type of information on behalf of an insurer.

---

[10] A.R.S. § 20-448.01(F) and (G).

Proposed Solution:

The consensus solution developed at the June 12 meeting is to recommend removing the redisclosure notice entirely from A.R.S. § 36-664(H) and A.R.S. § 20-448.01. Both statutes already require that a person who receives communicable disease or HIV-AIDS information may not disclose that information except as authorized by the statute. Removing the written redisclosure notice thus would not reduce any privacy protection available for this type of information.

We also recommend adding a permitted disclosure to an HIE. Because there is not a universally-recognized definition for a "health information exchange,"[11] we propose to define it as an agent that conducts health information exchange. We also propose to limit the disclosure to such agents that agree to limit disclosure to those purposes permitted by the statute, so that the information is protected "downstream."

We also recommend amending A.R.S. § 20-448.01and A.A.C. R20-6-1204 so that insurers may disclose HIV/AIDS in the same manner as providers. We recommend retaining those provisions essential to privacy protection of HIV/AIDS information handled by insurers, such as limitation of the type of information that may be released to an insurance medical information exchanges (which we redefine for clarity to ensure that it does not cover an HIE) and in responses to subpoenas or court orders.

We also recommend to the ADHS to remove the 180-day limit on authorization found in A.A.C. R20-6-1204.

36-664. Confidentiality; exceptions

A. A person who obtains communicable disease related information in the course of providing a health service or obtains that information from a health care provider pursuant to an authorization shall not disclose or be compelled to disclose that information except to the following:

1. The protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker.

2. The department or a local health department for purposes of notifying a good Samaritan pursuant to subsection E of this section.

3. An agent or employee of a health facility or health care provider to provide health services to the protected person or the protected person's child or for billing or reimbursement for health services.

4. A health facility or health care provider, in relation to the procurement, processing, distributing or use of a human body or a human body part, including organs, tissues, eyes, bones, arteries, blood, semen, milk or other body fluids, for use in medical education, research or therapy or for transplantation to another person.

5. A health facility or health care provider, or an organization, committee or individual designated by the

[11] The Office of the National Coordinator for Health Information Technology, for example, defines it as "the mobilization of healthcare information electronically across organizations within a region or community," not as an entity conducting that exchange.

health facility or health care provider, that is engaged in the review of professional practices, including the review of the quality, utilization or necessity of medical care, or an accreditation or oversight review organization responsible for the review of professional practices at a health facility or by a health care provider.

6. A private entity that accredits the health facility or health care provider and with whom the health facility or health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

7. A federal, state, county or local health officer if disclosure is mandated by federal or state law.

8. A federal, state or local government agency authorized by law to receive the information. The agency is authorized to redisclose the information only pursuant to this article or as otherwise permitted by law.

9. An authorized employee or agent of a federal, state or local government agency that supervises or monitors the health care provider or health facility or administers the program under which the health service is provided. An authorized employee or agent includes only an employee or agent who, in the ordinary course of business of the government agency, has access to records relating to the care or treatment of the protected person.

10. A person, health care provider or health facility to which disclosure is ordered by a court or administrative body pursuant to section 36-665.

11. The industrial commission or parties to an industrial commission claim pursuant to section 23-908, subsection D and section 23-1043.02.

12. Insurance entities pursuant to section 20-448.01 and third party payors or the payors' contractors.

13. Any person or entity as authorized by the patient or the patient's health care decision maker.

14. A person or entity as required by federal law.

15. The legal representative of the entity holding the information in order to secure legal advice.

16. A person or entity for research only if the research is conducted pursuant to applicable federal or state laws and regulations governing research.

17. AN AGENT FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE AGENT AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO DISCLOSE COMMUNICABLE-DISEASE RELATED INFORMATION ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. At the request of the department of economic security in conjunction with the placement of children in foster care or for adoption or court-ordered placement, a health care provider shall disclose communicable disease information, including HIV-related information, to the department of economic security.

C. A state, county or local health department or officer may disclose communicable disease related information if the disclosure is any of the following:

1. Specifically authorized or required by federal or state law.

2. Made pursuant to an authorization signed by the protected person or the protected person's health care decision maker.

3. Made to a contact of the protected person. The disclosure shall be made without identifying the

protected person.

4. For the purposes of research as authorized by state and federal law.

D. The director may authorize the release of information that identifies the protected person to the national center for health statistics of the United States public health service for the purposes of conducting a search of the national death index.

E. The department or a local health department shall disclose communicable disease related information to a good Samaritan who submits a request to the department or the local health department. The request shall document the occurrence of the accident, fire or other life-threatening emergency and shall include information regarding the nature of the significant exposure risk. The department shall adopt rules that prescribe standards of significant exposure risk based on the best available medical evidence. The department shall adopt rules that establish procedures for processing requests from good Samaritans pursuant to this subsection. The rules shall provide that the disclosure to the good Samaritan shall not reveal the protected person's name and shall be accompanied by a written statement that warns the good Samaritan that the confidentiality of the information is protected by state law.

F. An authorization to release communicable disease related information shall be signed by the protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker. An authorization shall be dated and shall specify to whom disclosure is authorized, the purpose for disclosure and the time period during which the release is effective. A general authorization for the release of medical or other information, including communicable disease related information, is not an authorization for the release of HIV-related information unless the authorization specifically indicates its purpose as an authorization for the release of confidential HIV-related information and complies with the requirements of this section.

G. A person to whom communicable disease related information is disclosed pursuant to this section shall not disclose the information to another person except as authorized by this section. This subsection does not apply to the protected person or a protected person's health care decision maker.

~~H. If a disclosure of communicable disease related information is made pursuant to an authorization under subsection F of this section, the disclosure shall be accompanied by a statement in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law.~~

~~I~~H. This section does not prohibit the listing of communicable disease related information, including acquired immune deficiency syndrome, HIV-related illness or HIV infection, in a certificate of death, autopsy report or other related document that is prepared pursuant to law to document the cause of death or that is prepared to release a body to a funeral director. This section does not modify a law or rule relating to access to death certificates, autopsy reports or other related documents.

~~J~~I. If a person in possession of HIV-related information reasonably believes that an identifiable third party is at risk of HIV infection, that person may report that risk to the department. The report shall be in writing and include the name and address of the identifiable third party and the name and address of the person making the report. The department shall contact the person at risk pursuant to rules adopted by the department. The department employee making the initial contact shall have expertise in counseling persons who have been exposed to or tested positive for HIV or acquired immune deficiency syndrome.

~~K~~J. Except as otherwise provided pursuant to this article or subject to an order or search warrant issued pursuant to section 36-665, a person who receives HIV-related information in the course of providing a health service or pursuant to a release of HIV-related information shall not disclose that information to another person or legal entity or be compelled by subpoena, order, search warrant or other judicial process to disclose that information to another person or legal entity.

~~L~~K. This section and sections 36-663, 36-666, 36-667 and 36-668 do not apply to persons or entities subject to regulation under title 20.

20-448.01. Required insurance procedures relating to HIV information; confidentiality; violations; penalties; definitions

A. In this section unless the context otherwise requires:

1. "Confidential HIV-related information" means information concerning whether a person has had an HIV-related test or has HIV infection, HIV-related illness or acquired immune deficiency syndrome and includes information which identifies or reasonably permits identification of that person or the person's contacts.

2. "HIV" means the human immunodeficiency virus.

3. "HIV-related test" means a laboratory test or series of tests for the virus, components of the virus or antibodies to the virus thought to indicate the presence of HIV infection.

4. "Protected person" means a person who takes an HIV-related test or who has been diagnosed as having HIV infection, acquired immune deficiency syndrome or HIV-related illness.

5. "Person" includes all entities subject to regulation under title 20, the employees, contractors and agents thereof, and anyone performing insurance related tasks for such entities, employees, contractors or agents.

B. Except as otherwise specifically authorized or required by this state or by federal law, no person may require the performance of, or perform an HIV-related test without first receiving the specific written informed consent of the subject of the test who has capacity to consent or, if the subject lacks capacity to consent, of a person authorized pursuant to law to consent for that person. Written consent shall be in a form as prescribed by the director.

C. No person who obtains confidential HIV-related information in the course of processing insurance information or insurance applications or pursuant to a release of confidential HIV-related information may disclose or be compelled to disclose that information except AS PERMITTED IN SECTION 36-664, EXCEPT THAT IN A RELEASE OF INFORMATION TO A CONSUMER REPORTING AGENCY OR OTHER ORGANIZATION WHOSE PURPOSE IS TO DETECT FRAUD IN INSURANCE, SUCH AS THE MEDICAL INFORMATION BUREAU: ~~to the following:~~

~~1. The protected person or, if the protected person lacks capacity to consent, a person authorized pursuant to law to consent for the protected person.~~

~~2. A person to whom disclosure is authorized in writing pursuant to a release as set forth in subsection E of this section, including but not limited to a physician designated by the insured or a medical information exchange for insurers operated under procedures intended to ensure confidentiality, provided that1.~~

~~1. In the case of a medical information exchang~~e:

~~(a)~~ 1. The insurer will not report that blood tests of an applicant showed the presence of the AIDS virus antibodies, but only that unspecified blood test results were abnormal.

~~(b)~~ 2. Reports must use a general code that also covers results of tests for many diseases or conditions, such as abnormal blood counts that are not related to HIV, AIDS, AIDS related complex or similar diseases.

~~3. A government agency specifically authorized by law to receive the information. The agency is~~

~~authorized to redisclose the information only pursuant to this section or as otherwise permitted by law.~~

~~42. A person regulated by this title to which disclosure is ordered by a court or administrative body ONLY pursuant to section 36-665.~~

~~5. The industrial commission or parties to an industrial commission claim pursuant to the provisions of section 23-908, subsection D and section 23-1043.02.~~

D. Test results and application responses may be shared with the underwriting departments of the insurer and reinsurers, or to those contractually retained medical personnel, laboratories, and insurance affiliates, excluding agents and brokers, which are involved in underwriting decisions regarding the individual's application if disclosure is reasonably necessary to make the underwriting decision regarding such application, and claims information may be shared with claims personnel and attorneys reviewing claims if disclosure is reasonably necessary to process and resolve claims.

E. A release of confidential HIV-related information pursuant to subsection C, paragraph 2 of this section shall be signed by the protected person or, if the protected person lacks capacity to consent, a person authorized pursuant to law to consent for the protected person. A release shall be dated and shall specify to whom disclosure is authorized, the purpose for disclosure and the time period during which the release is effective. A general authorization for the release of medical or other information is not a release of confidential HIV-related information unless the authorization specifically indicates its purpose as a general authorization and an authorization for the release of confidential HIV-related information and complies with the requirements of this section.

F. A person to whom confidential HIV-related information is disclosed pursuant to this section shall not disclose the information to another person except as authorized by this section. This subsection does not apply to the protected person or a person who is authorized pursuant to law to consent for the protected person.

~~G. If a disclosure of confidential HIV-related information is made pursuant to the provisions of a written release as permitted by subsection C, paragraph 2 of this section, the disclosure shall be accompanied by a statement in writing which warns that the information is from confidential records which are protected by state law that prohibits further disclosure of the information without the specific written consent of the person to whom it pertains or as otherwise permitted by law.~~

~~H. The person making a disclosure in accordance with subsection C, paragraphs 3, 4 and 5, and subsection G of this section shall keep a record of all disclosures for the time period prescribed by the director. On request, a protected person or his legal representative shall have access to the record.~~

~~I~~G. Except as otherwise provided pursuant to this section or subject to an order or search warrant issued pursuant to section 36-665, no person who receives confidential HIV-related information pursuant to a release of confidential HIV-related information may disclose that information to another person or legal entity or be compelled by subpoena, order, search warrant or other judicial process to disclose that information to another person or legal entity.

~~J~~H. The director shall adopt rules to implement the allowable tests and testing procedures, written consent to perform a human immunodeficiency virus relate test, procedures for confidentiality and disclosure of medical information and procedures for gathering underwriting information and may adopt additional rules reasonable and necessary to implement this section.

~~K~~I. Notwithstanding any other provision of law to the contrary, nothing in this section shall be interpreted to restrict the director's authority to full access to records of any entity subject to regulation under title 20, including but not limited to all records containing confidential HIV-related information. The director may only redisclose confidential HIV-related information in accordance with this section.

~~L~~J. A protected person, whose rights provided in this section have been violated by a person or entity

described in subsection A, paragraph 5 of this section, has those individual remedies specified in section 20-2118 against such a person or entity.

R20-6-1204. Release of Confidential HIV-related Information; Release Form

A. ~~Except as required by law or authorized pursuant to a written consent to be tested, a~~An insurer shall ~~not~~ disclose confidential HIV-related information ONLY AS PERMITTED BY ARIZONA REVISED STATUTES SECTION 20-448.01~~01to any person unless a written release form is executed by the applicant or, if the applicant lacks legal capacity to consent to such release, by a person authorized by law to consent to the release of information on behalf of the applicant. The applicant or the applicant's legal representative shall be entitled to receive a copy of the release. A photocopy shall be as valid as the original~~.

B. The applicant or the applicant's legal representative shall be entitled to receive a copy of the release FOR CONFIDENTIAL HIV-RELATED INFORMATION. A photocopy shall be as valid as the original .Such written release form shall contain the following information:
1. The name and address of the person to whom the information shall be disclosed;
2. The specific purpose for which disclosure is to be made; and
~~3. The time period during which the written release is to be effective but in no case shall such time period exceed 180 days from the date the release is signed by the applicant or the applicant's legal representative;~~
~~4~~3. The signature of the applicant or of the person authorized by law to consent to such release, and the date the release form was signed.

(2) Mental Health Information:

A.R.S. § 36-501, *et seq*.

Description of Laws:

The Arizona mental health statutes have special restrictions on the disclosure of mental health information.[12] These statutes have limited applicability, however, and apply only to mental health providers and health care institutions licensed as behavioral health providers, including those providing inpatient and outpatient mental health services.[13] A "mental health provider" includes physicians and other providers of mental health or behavioral health services who are involved in evaluating, caring for, treating or rehabilitating a patient.[14] Health care providers that provide mental or behavioral health services but who are not licensed as behavioral health providers, such as hospital emergency departments that provide psychiatric consultations, are not subject to Arizona mental health statutes and regulations.

Information contained in mental health records is confidential and may be released only as expressly permitted by the statute.[15] (The HIPAA Privacy Rule also contains

[12] A.R.S. § 36-501 et seq.

[13] A.R.S. § 36-501(19).

[14] A.R.S. § 36-501(27).

[15] A.R.S. § 36-509

additional restrictions on the use and disclosure of "psychotherapy notes"—the mental health care professional's personal notes kept separate from the regular medical record.[16])

Identified Barriers to Health Information Exchange:

A.R.S. § 36-509(14) permits disclosure to a "third party payor or the payor's contractor to obtain reimbursement for health care, mental health care or behavioral health care provided to the patient." The consensus position developed at the June 12 meeting is that this is not broad enough to facilitate the use of information in the HIE for such purposes as case management, disease management, and other treatment-related functions that are necessary for behavioral health care.

Moreover, A.R.S. § 36-509 could be interpreted as not permitting direct disclosure of information to an HIE; the statute expressly lists permitted disclosures, which do not include an HIE.

Proposed Solution:

We recommend amending the statute to permit disclosure to third party payors or the payor's contractor for "payment," as defined under the HIPAA Privacy Rule. We also recommend expressly permitting disclosure to an HIE.

36-509. Confidential records

A. A health care entity must keep records and information contained in records confidential and not as public records, except as provided in this section. Records and information contained in records may only be disclosed to:

1. Physicians and providers of health, mental health or social and welfare services involved in caring for, treating or rehabilitating the patient.

2. Individuals to whom the patient or the patient's health care decision maker has given authorization to have information disclosed.

3. Persons authorized by a court order.

4. Persons doing research only if the activity is conducted pursuant to applicable federal or state laws and regulations governing research.

5. The state department of corrections in cases in which prisoners confined to the state prison are patients in the state hospital on authorized transfers either by voluntary admission or by order of the court.

6. Governmental or law enforcement agencies if necessary to:

(a) Secure the return of a patient who is on unauthorized absence from any agency where the patient was undergoing evaluation and treatment.

[16] 45 C.F.R. § 164.501.

(b) Report a crime on the premises.

(c) Avert a serious and imminent threat to an individual or the public.

7. Persons, including family members, actively participating in the patient's care, treatment or supervision. A health care provider may only release information relating to the patient's diagnosis, prognosis, need for hospitalization, anticipated length of stay, discharge plan, medication, medication side effects and short-term and long-term treatment goals. A health care provider may make this release only after the treating professional or that person's designee interviews the patient or the patient's health care decision maker and the patient or the patient's health care decision maker does not object, unless federal or state law permits the disclosure. If the patient does not have the opportunity to object to the disclosure because of incapacity or an emergency circumstance and the patient's health care decision maker is not available to object to the release, the health care provider in the exercise of professional judgment may determine if the disclosure is in the best interests of the patient and, if so, may release the information authorized pursuant to this paragraph. A decision to release or withhold information is subject to review pursuant to section 36-517.01. The health care provider must record the name of any person to whom any information is given under this paragraph.

8. A state agency that licenses health professionals pursuant to title 32, chapter 13, 15, 17, 19.1 or 33 and that requires these records in the course of investigating complaints of professional negligence, incompetence or lack of clinical judgment.

9. A state or federal agency that licenses health care providers.

10. A governmental agency or a competent professional, as defined in section 36-3701, in order to comply with chapter 37 of this title.

11. Human rights committees established pursuant to title 41, chapter 35. Any information released pursuant to this paragraph shall comply with the requirements of section 41-3804 and applicable federal law and shall be released without personally identifiable information unless the personally identifiable information is required for the official purposes of the human rights committee. Case information received by a human rights committee shall be maintained as confidential. For the purposes of this paragraph, "personally identifiable information" includes a person's name, address, date of birth, social security number, tribal enrollment number, telephone or telefacsimile number, driver license number, places of employment, school identification number and military identification number or any other distinguishing characteristic that tends to identify a particular person.

12. A patient or the patient's health care decision maker pursuant to section 36-507.

13. The department of public safety by the court to comply with the requirements of section 36-540, subsection N.

14. A third party payor or the payor's contractor FOR PAYMENT PURPOSES, AS DEFINED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 160 AND PART 164, SUBPART E)~~to obtain reimbursement for health care, mental health care or behavioral health care provided to the patient~~.

15. A private entity that accredits the health care provider and with whom the health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

16. The legal representative of a health care entity in possession of the record for the purpose of securing legal advice.

17. A person or entity as otherwise required by state or federal law.

18. A person or entity as permitted by the federal regulations on alcohol and drug abuse treatment (42 Code of Federal Regulations part 2).

19. A person or entity to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

20. A person maintaining health statistics for public health purposes as authorized by law.

21. A grand jury as directed by subpoena.

22. AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO DISCLOSE RECORDS AND INFORMATION CONTAINED IN RECORDS ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. Information and records obtained in the course of evaluation, examination or treatment and submitted in any court proceeding pursuant to this chapter or title 14, chapter 5 are confidential and are not public records unless the hearing requirements of this chapter or title 14, chapter 5 require a different procedure. Information and records that are obtained pursuant to this section and submitted in a court proceeding pursuant to title 14, chapter 5 and that are not clearly identified by the parties as confidential and segregated from nonconfidential information and records are considered public records.

C. Notwithstanding subsections A and B of this section, the legal representative of a patient who is the subject of a proceeding conducted pursuant to this chapter and title 14, chapter 5 has access to the patient's information and records in the possession of a health care entity or filed with the court.

(3) Immunization Information:

A.R.S. § 36-135 and A.A.C. R9-6-708

Description of Laws:

A.R.S. § 36-135 and A.A.C. R9-6-708 restrict the purposes for which ADHS may release immunization data. Specifically, A.R.S. § 36-135(D) permits ADHS to release identifying information contained in immunization data "only to the child's health care professional, parent, guardian, health care service organization, the Arizona health care cost containment system and its providers as defined in title 36, chapter 29, or a school official who is authorized by law to receive and record immunization records."[17] ADHS also "may, by rule, release immunization information to persons for a specified purpose."[18]

A.A.C. R9-6-708 additionally permits ADHS to release immunization information to: (1) an authorized representative of a state or local health agency for the control, investigation, analysis, or follow-up of disease; (2) a child care administrator, to determine the immunization status of a child in the child care; (3) an authorized representative of WIC, to determine the immunization status of a child enrolled in WIC; (4) an individual or organization authorized by the Department, to conduct medical

[17] A.R.S. § 36-135(D).

[18] Id.

research to evaluate medical services and health related services, health quality, immunization data quality, and efficacy; or (5) an authorized representative of an out-of-state agency, including a state health department, local health agency, school, child care, health care provider, or a state agency that has legal custody of a child.

A.R.S. § 36-135(E) additionally specifies that information in the ADHS immunization data system is confidential and that "a person who is authorized to receive confidential information under subsection D shall not disclose this information to any other person" Substantial penalties are in place for violating these confidentiality provision: (1) "A health care professional who does not comply with the requirements of this section violates a law or task applicable to the practice of medicine and an act of unprofessional conduct";[19] and (2) "any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor."[20]

Identified Barriers to Health Information Exchange:

Many physicians believe it would be useful to have immunization information in an HIE, as patients often do not recall or retain this information in their records. If an HIE will be populated with immunization data from ADHS, rather than directly from health care providers, the immunization statute and ADHS regulations may pose the following barriers to including this information in the HIE.

First, and most significantly, the statute specifies that "a person who is authorized to receive confidential information under subsection D shall not disclose this information to any other person." This provision would prohibit HIEs from handling immunization information received from ADHS, despite the value immunization information has for patient care. This provision would also prohibit providers from releasing immunization information to an HIE if the providers received that information from ADHS.

Second, A.R.S. § 36-135 and A.A.C. R9-6-708 permit release of information to AHCCCS and "health care services organizations" (HMOs), but not other insurers. While Arizona HIEs have not determined yet whether and when insurers will have access to information in an HIE, this provision's distinction between HMOs and other insurers may interfere with the participation of some insurers in valuable exchange efforts.

Next, to the extent that information handled by an HIE will be utilized for research purposes (of course, only with approval by an Institutional Review Board and pursuant to all applicable federal regulations governing human subject research), the regulations permit ADHS to release information only for health services research, not other types of research.

[19] A.R.S. § 36-135(G).

[20] A.R.S. § 36-135(H).

Finally, A.R.S. § 36-135 would not permit ADHS to release immunization information directly to an HIE.

3. Proposed Solution:

The consensus at the June 12 meeting was to remove the absolute prohibition against redisclosure of immunization information, and instead to provide that immunization information may be redisclosed as permitted by A.R.S. § 36-135 and A.A.C. R9-6-708. This will continue to restrict who receives immunization information, but will not interfere with the exchange of immunization information for treatment and other permitted purposes.

We also recommend clarifying that disclosures to health plans are not restricted to AHCCCS and HMOs, and permitting ADHS to release immunization information directly to an HIE.

For regulatory changes, we recommend expanding the types of permissible research.

36-135. Child immunization reporting system; requirements; access; confidentiality; immunity; violation; classification

A. The child immunization reporting system is established in the department to collect, store, analyze, release and report immunization data.

B. Beginning on January 1, 1998, a health care professional who is licensed under title 32 to provide immunizations shall, except as provided in subsection I, report the following information:

1. The health care professional's name, business address and business telephone number.

2. The child's name, address, the child's social security number if known and not confidential, gender, date of birth and mother's maiden name.

3. The type of vaccine administered and the date it is administered.

C. The health care professional may submit this information to the department on a weekly or monthly basis by telephone, facsimile, mail, computer or any other method prescribed by the department.

D. Except as provided in subsection I, the department shall release identifying information only to the child's health care professional, parent, guardian, AN ENTITY REGULATED UNDER TITLE 20 ~~health care service organization~~, the Arizona health care cost containment system and its providers as defined in title 36, chapter 29, ~~or~~ a school official who is authorized by law to receive and record immunization records, OR AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF IDENTIFYING INFORMATION AND TO DISCLOSE IDENTIFYING INFORMATION ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION. The department may, by rule, release immunization information to persons for a specified purpose. The department may release nonidentifying summary statistics.

E. Identifying information in the system is confidential. A person who is authorized to receive confidential information under subsection D OR DEPARTMENT RULE shall ~~not~~ disclose this information ~~to any other person~~ ONLY AS PERMITTED BY THIS SECTION OR DEPARTMENT RULE.

F. A health care professional who provides information in good faith pursuant to this section is not subject to civil or criminal liability.

G. A health care professional who does not comply with the requirements of this section violates a law or task applicable to the practice of medicine and an act of unprofessional conduct.

H. Any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor.

I. At the request of the child's parent or guardian, the department of health services shall provide a form to be signed that allows confidential immunization information to be withheld from all persons including persons authorized to receive confidential information pursuant to subsection D. If the request is delivered to the health care professional prior to the immunization, the health care professional shall not forward the information required under subsection B to the department.

(4) Genetic Testing Information:
A.R.S. § 12-2801, *et seq.* and A.R.S. § 20-448.02, *et seq.*

Description of the Laws:

Arizona law contains significant restrictions on disclosure of genetic testing and information derived from genetic testing, due to the heightened concern with the potential for discrimination in employment and insurance if information related to genetic predisposition to disease is released. On the other hand, genetic testing information is becoming increasingly significant information for diagnosis and effective treatment as the industry develops "personalized medicine"; information about the genetics of a particular cancer tumor or the ability to metabolize warfarin, for example, may make a significant difference in what treatment is provided to a particular patient.

A.R.S. § 12-2801, *et seq.*, protects "genetic testing and information derived from genetic testing." Genetic testing includes "a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies, including carrier status, that: (i) Are linked to physical or mental disorders or impairments; (ii) Indicate a susceptibility to any illness, disease, impairment or other disorder, whether physical or mental; or (iii) Demonstrate genetic or chromosomal damage due to any environmental factor."[21] The phrase "information derived from genetic testing" is not defined.

The statute permits disclosure without authorization only to the patient and the patient's health care decision maker, the patient's health care provider, researchers (if federal confidentiality requirements are followed), organ procurement agencies and the state registries, and permits limited internal uses by the provider.[22] In addition, the

[21] Id. Genetic testing does not include: "(i) Chemical, blood and urine analyses that are widely accepted and used in clinical practice and that are not used to determine genetic traits; (ii) Tests used in a criminal investigation or prosecution or as a result of a criminal conviction; (iii) Tests for the presence of the human immunodeficiency virus; (iv) Tests to determine paternity conducted pursuant to title 25, chapter 6, article 1; or (v) Tests given for use in biomedical research that is conducted to generate scientific knowledge about genes or to learn about the genetic basis of disease or for developing pharmaceutical and other treatment of disease." A.R.S. § 12-2801.

22 See A.R.S. § 12-2802(A).

statute prohibits a person holding genetic testing and information derived from genetic testing from producing that information pursuant to a subpoena in a manner that allows identification of the person tested, unless the disclosure otherwise falls within the eleven permitted uses and disclosures listed in the statute.[23] Importantly, the statute applies to any person who receives genetic testing information: "[A] person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person."[24]

Health care organizations that are subject to regulation by the Arizona Department of Insurance also must comply with A.R.S. § 20-448.02. This statute requires an insurance company to obtain written informed consent for genetic testing, and prohibits release of the genetic testing results to anyone without the express consent of the person tested.[25] (A.R.S. § 12-2802 provides that it does not affect the title 20 provisions governing insurance entities' handling of genetic testing information.)

Identified Legal Barriers to Health Information Exchange**:**

The phrase "information derived from genetic testing" in A.R.S. § 12-2801 is not defined; an individual involved in drafting the statute has explained that this phrase was intended to cover genetic testing results and reports of those results, but not diagnosis of a disease or treatment for a disease. Indeed, if "information derived from genetic testing" were to include the diagnosis of a genetically-based disease or treatment for such a disease, it would be exceedingly difficult for providers to segregate that information from the rest of the record. Difficulty in segregating information would have the effect of preventing providers from engaging in HIE.

We also noted confusion about when disclosures are permitted to health care providers. A.R.S. § 12-2802(6) permits disclosure to an agent or employee of a health care provider only if: (a) The health care provider performs the test or is authorized to obtain the test results by the person tested for the purposes of genetic counseling or treatment; (b) The agent or employee provides patient care, treatment or counseling; and (c) The agent or employee needs to know the information in order to conduct the test or provide patient care, treatment or counseling. On the other hand, subsection (11) permits disclosures to a "health care provider that assumes the responsibility to provide care for, or consultation to, the patient from another health care provider that had access to the patient's genetic records"—in other words, to a treating provider (without the restrictions set forth in subsection (6). Confusion about when disclosures to treating providers are permitted may interfere with HIE.

---

[23] A.R.S. § 12-2802(B) – (C).

[24] A.R.S. § 12-2802(F).

[25] A genetic test in the insurance statute is similarly defined as "an analysis of an individual's DNA, gene products or chromosomes that indicates a propensity for or susceptibility to illness, disease, impairment or other disorders, whether physical or mental, or that demonstrates genetic or chromosomal damage due to environmental factors, or carrier status for disease or disorder." A.R.S. § 20-448.02.

A.R.S. § 12-2802(F) applies to any person who receives genetic testing, and provides that "a person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person." This phrase would prevent providers who receive genetic testing information from releasing it to an HIE or directly to other providers for treatment purposes.

Finally, A.R.S. § 20-448.02 requires an insurance company from releasing genetic testing results to anyone without the express consent of the person tested, including to a treating provider or to an HIE.

Proposed Solution:

We recommend that A.R.S. § 12-2801 be amended to clarify that "information derived from genetic testing" was not intended to cover diagnosis of a disease or treatment for a disease. We also recommend amending A.R.S. § 12-2802 to clarify that disclosure to treating providers are permitted, and to remove the redisclosure prohibition and instead permit disclosures that otherwise are permitted under the statute. We also recommend adding disclosures to an HIE as a permissible disclosure.

Finally, we recommend amending the insurance statute, A.R.S. § 20-448.02, to permit disclosures in the same instances as A.R.S. § 12-2802. This will permit insurers to contribute this information to an HIE, as well.

12-2801. Definitions

In this chapter, unless the context otherwise requires:

1. "Genetic test" or "genetic testing":

(a) Means a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies, including carrier status, that:

(i) Are linked to physical or mental disorders or impairments.

(ii) Indicate a susceptibility to any illness, disease, impairment or other disorder, whether physical or mental.

(iii) Demonstrate genetic or chromosomal damage due to any environmental factor.

(b) Does not include:

(i) Chemical, blood and urine analyses that are widely accepted and used in clinical practice and that are not used to determine genetic traits.

(ii) Tests used in a criminal investigation or prosecution or as a result of a criminal conviction.

(iii) Tests for the presence of the human immunodeficiency virus.

(iv) Tests to determine paternity conducted pursuant to title 25, chapter 6, article 1.

(v) Tests given for use in biomedical research that is conducted to generate scientific knowledge about genes or to learn about the genetic basis of disease or for developing pharmaceutical and other treatment of disease.

2. "Health care decision maker" means a person who is authorized to make health care treatment decisions for the patient, including a parent of a minor and a person who is authorized to make these decisions pursuant to title 14, chapter 5, article 2 or 3 or section 8-514.05, 36-3221, 36-3231 or 36-3281.

3. "Health care provider" means physicians licensed pursuant to title 32, chapter 13 or 17, physician assistants licensed pursuant to title 32, chapter 25, registered nurse practitioners licensed pursuant to title 32, chapter 15, health care institutions as defined in section 36-401 and clinical laboratories licensed pursuant to title 36, chapter 4.1.

4. "INFORMATION DERIVED FROM GENETIC TESTING" IS INFORMATION ABOUT THE RESULTS OF A GENETIC TEST AND DOES NOT INCLUDE INFORMATION RELFECTING A DIAGNOSIS OF OR TREATMENT FOR A DISEASE.

12-2802. Confidentiality of genetic testing results; disclosure

A. Except as otherwise provided in this article, genetic testing and information derived from genetic testing are confidential and considered privileged to the person tested and shall be released only to:

1. The person tested.

2. Any person who is specifically authorized in writing by the person tested or by that person's health care decision maker to receive this information.

3. The health care decision maker of the person tested.

4. A researcher for medical research or public health purposes only if the research is conducted pursuant to applicable federal or state laws and regulations governing clinical and biological research or if the identity of the individual providing the sample is not disclosed to the person collecting and conducting the research.

5. A third person if approved by a human subjects review committee or a human ethics committee, with respect to persons who are subject to an Arizona cancer registry OR OTHER DISEASE REGISTRY.

~~6. An authorized agent or employee of a health care provider if all of the following are true:~~

~~(a) The health care provider performs the test or is authorized to obtain the test results by the person tested for the purposes of genetic counseling or treatment.~~

~~(b) The agent or employee provides patient care, treatment or counseling.~~

~~(c) The agent or employee needs to know the information in order to conduct the test or provide patient care, treatment or counseling.~~

~~7~~6. A health care provider that procures, processes, distributes or uses:

(a) A human body part from a deceased person with respect to medical information regarding that person.

(b) Semen or ova for the purpose of artificial insemination.

~~8~~7. A health care provider to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

~~9~~8. The authorized agent of a federal, state or county health department to conduct activities specifically authorized pursuant to the laws of this state for the birth defects registry, children's rehabilitative services, newborn screening and sickle cell diagnosis and treatment programs and chronic, environmentally provoked and infectious disease programs.

~~10~~9. To obtain legal advice, the legal representative of a health care provider that is in possession of the medical record.

~~11~~10. A health care provider that assumes the responsibility to provide care for, or consultation to, the patient ~~from another health care provider that had access to the patient's genetic records~~.

11. AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO DISCLOSE GENETIC TESTING AND INFORMATION DERIVED FROM GENETIC TESTING ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. A person shall not disclose or be compelled to disclose the identity of any person on whom a genetic test is performed or the results of a genetic test in a manner that allows identification of the person tested except to the persons specified in the circumstances set forth in subsection A of this section.

C. If genetic testing information is subpoenaed, a health care provider shall respond pursuant to section 12-2294.01, subsection E. In determining whether to order production of the genetic testing information, the court shall take all steps necessary to prevent the disclosure or dissemination of that information.

D. Except as provided in this section, chapter 13, article 7.1 of this title does not apply to GENETIC TESTING OR INFORMATION DERIVED FROM genetic testing ~~information~~ that is contained within a patient's medical record.

E. Following the death of a person who had genetic testing performed, the release of the testing information is governed by section 12-2294, subsection D, except that the person may deny, release or limit release of the genetic testing results by adopting a provision in a testamentary document.

F. Except as specifically provided in this article, a person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person EXCEPT AS PROVIDED IN THIS SECTION.

G. A health care provider and the provider's agents and employees that act in good faith and that comply with this article are not subject to civil liability. The good faith of a health care provider that complies with this article is presumed. The presumption may be rebutted by a preponderance of the evidence.

H. This article does not limit the effect of title 20 provisions governing the confidentiality and use of genetic testing information.

20-448.02. Genetic testing; informed consent; definitions

A. Except as otherwise specifically authorized or required by this state or by federal law, a person shall not require the performance of or perform a genetic test without first receiving the specific written informed consent of the subject of the test who has the capacity to consent or, if the person subject to the test lacks the capacity to consent, of a person authorized pursuant to law to consent for that person. Written consent shall be in a form as prescribed by the director. The results of a genetic test performed pursuant to this subsection are privileged and confidential and may not be released to any party, ~~without the expressed consent of the subject of the test~~. EXCEPT AS PERMITTED IN ARIZONA REVISED STATUTES, SECTION 12-2802.

B. As used in this section:

1. "Gene products" means gene fragments, nucleic acids or proteins derived from deoxyribonucleic acids that would be a reflection of or indicate DNA sequence information.

2. "Genetic test" means an analysis of an individual's DNA, gene products or chromosomes that indicates a propensity for or susceptibility to illness, disease, impairment or other disorders, whether physical or mental, or that demonstrates genetic or chromosomal damage due to environmental factors, or carrier status for disease or disorder.

(5) Medical Records Subpoena Statute

A.R.S. § 12-2294.01

Description of Laws:

The medical records subpoena statute, A.R.S. § 12-2294.01, governs how "health care providers" may produce medical records and payment records in response to subpoenas. "Health care providers" include licensed health care professionals that maintain medical records, health care institutions, ambulance services, and HMOs. The statute generally requires a patient to sign an authorization before releasing medical or payment records pursuant to a subpoena, but there are various exceptions in the statute. (See below.)

Identified Barriers to Health Information Exchange:

The current medical records subpoena statute poses three potential barriers to health care providers' participation in HIE if not clarified: (1) how do providers' handle other providers' records and HIE records in their responses to subpoenas; (2) how are subpoenas issued to an HIE *itself* handled; and (3) how are depositions of record custodians handled?

(1) Treatment of records from other sources: An increasing number of patients are presenting to hospitals and physicians with medical records from the patient's other health care providers, often stored on CDs or in other electronic form. Moreover, providers will begin to have access to information in HIE systems. The specific question presented is when records from other sources should be treated as the provider's own medical record in responding to subpoenas.

Right now, the definition of "medical records" in Arizona includes "all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers." A.R.S. § 12-2291. We believe this definition is too broad and should instead reflect the industry standard. The industry standard, as reflected in AHIMA guidance documents, treats records from other providers as not being a part of the medical record

produced in response to a subpoena unless the other providers' records are used by the responding provider in the provision of patient care.[26]

(2) Subpoenas issued to the HIE: The present medical records subpoena statute applies only to "health care providers" as defined above. It does not apply to HIEs or other third parties that hold medical records or payment records on behalf of health care providers. This may pose a barrier to health care providers' participation in an HIE—some may be wary of entrusting their patients' health information to an HIE unless the HIE has the same protections as the health care providers in responding to a subpoena.

(3) Depositions of Custodians of Record: We also suggest refining the subpoena statute to clarify when health care providers and HIEs must submit their custodians of record for a deposition. Hospitals and other health care providers long have followed the practice of providing copies of subpoenaed medical records with an affidavit from the custodian of records that the copy provided is a true and complete copy. Hospitals and other providers have followed that practice so that their custodians of records do not have to be deposed to establish the admissibility of the records produced. Unfortunately, hospitals have received notices of depositions of their custodian of records, even though they provided the affidavit to establish admissibility. This is a large resource commitment—providers are required to pay their employee to attend the deposition as well as a lawyer to represent the employee in the deposition—and this resource commitment is not necessary to establish admissibility of the records. This will be an equally large, and unnecessary, resource commitment for developing HIEs, as well.

Proposed Solutions:

First, to deal with the treatment of medical records from other sources, the Legal Working Group proposes a change in the definition of "medical record" in A.R.S. § 12-2291, to indicate that records from other sources are part of a provider's medical record only if they are used for the provision of patient care. This new language would reflect the national standard that records received from other sources (whether other health care providers, an HIE, or the patient's personal health record), would only be a part of the provider's own medical record if the provider uses those records to provide care to the patient.

Second, we recommend that the existing subpoena statute be extended to HIEs and others that hold records on behalf of health care providers, which would provide sufficient protection for the privacy of the health information held or managed by HIEs. We favor extending the statute to any third parties that hold or manage health information on behalf of health care providers, as this would also provide protection for vendors other than HIEs that hold or manage health information on behalf of health care providers.

[26] Id.

Third, we propose a formal process to submit an affidavit in support of records produced, as well as clarify that providers are not required to submit their custodian of records for deposition if they provide a compliant affidavit.

12-2291. Definitions

In this article, unless the context otherwise requires:

1. "Contractor" means an agency or service that duplicates medical records on behalf of health care providers.

2. "Department" means the department of health services.

3. "Health care decision maker" means an individual who is authorized to make health care treatment decisions for the patient, including a parent of a minor or an individual who is authorized pursuant to section 8-514.05, title 14, chapter 5, article 2 or 3 or section 36-3221, 36-3231 or 36-3281.

4. "Health care provider" means:

(a) A person who is licensed pursuant to title 32 and who maintains medical records.

(b) A health care institution as defined in section 36-401.

(c) An ambulance service as defined in section 36-2201.

(d) A health care services organization licensed pursuant to title 20, chapter 4, article 9.

5. "Medical records" means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment BY THE HEALTH CARE PROVIDER, including medical records that are prepared by a health care provider or RECEIVED FROM ~~by~~ other providers THAT ARE USED IN THE PROVISION OF PATIENT CARE BY THE HEALTH CARE PROVIDER. Medical records do not include materials that are prepared in connection with utilization review, peer review or quality assurance activities, including records that a health care provider prepares pursuant to section 36-441, 36-445, 36-2402 or 36-2917. Medical records do not include recorded telephone and radio calls to and from a publicly operated emergency dispatch office relating to requests for emergency services or reports of suspected criminal activity, but shall include communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the diagnosis or treatment of a person.

6. "Payment records" means all communications related to payment for a patient's health care that contain individually identifiable information.

7. "Source data" means information that is summarized, interpreted or reported in the medical record, including x-rays and other diagnostic images.

12-2294.01. Release of medical records or payment records to third parties pursuant to subpoena

A. A subpoena seeking medical records or payment records shall be served on the health care provider and any party to the proceedings at least ten days before the production date on the subpoena.

B. A subpoena that seeks medical records or payments records must meet one of the following requirements:

1. The subpoena is accompanied by a written authorization signed by the patient or the patient's health care decision maker.

2. The subpoena is accompanied by a court or tribunal order that requires the release of the records to the party seeking the records or that meets the requirements for a qualified protective order under the health insurance portability and accountability act privacy standards (42 Code of Federal Regulations section 164.512(e)).

3. The subpoena is a grand jury subpoena issued in a criminal investigation.

4. The subpoena is issued by a health profession regulatory board as defined in section 32-3201.

5. The health care provider is required by another law to release the records to the party seeking the records.

C. If a subpoena does not meet one of the requirements of subsection B of this section, a health care provider shall not produce the medical records or payment records to the party seeking the records, but may either file the records under seal pursuant to subsection D of this section, object to production under subsection E of this section or file a motion to quash or modify the subpoena under rule 45 of the Arizona rules of civil procedure.

D. It is sufficient compliance with a subpoena issued in a court or tribunal proceeding if a health care provider delivers the medical records or payment records under seal as follows:

1. The health care provider may deliver by certified mail or in person a copy of all the records described in the subpoena by the production date to the clerk of the court or tribunal or if there is no clerk then to the court or tribunal, together with the affidavit described in paragraph 4 of this subsection.

2. The health care provider shall separately enclose and seal a copy of the records in an inner envelope or wrapper, with the title and number of the action, name of the health care provider and date of the subpoena clearly inscribed on the copy of the records. The health care provider shall enclose the sealed envelope or wrapper in an outer envelope or wrapper that is sealed and directed to the clerk of the court or tribunal or if there is no clerk then to the court or tribunal.

3. The copy of the records shall remain sealed and shall be opened only on order of the court or tribunal conducting the proceeding.

4. The records shall be accompanied by the affidavit of the custodian or other qualified witness, stating in substance each of the following:

(a) That the affiant is the duly authorized custodian of the records and has authority to certify the records.

(b) That the copy is a true complete copy of the records described in the subpoena.

(c) If applicable, that the health care provider is subject to the confidentiality requirements in 42 United States Code sections 290dd-3 and 290ee-3 and applicable regulations and that those confidentiality requirements may apply to the requested records. The affidavit shall request that the court make a determination, if required under applicable federal law and regulations, as to the confidentiality of the records submitted.

(d) If applicable, that the health care provider has none of the records described or only part of the records described in the subpoena.

5. The copy of the records is admissible in evidence as provided under rule 902(11), Arizona rules of evidence. The affidavit is admissible as evidence of the matters stated in the affidavit and the matters stated are presumed true. If more than one person has knowledge of the facts, more than one affidavit

may be made. The presumption established by this paragraph is a presumption affecting the burden of producing evidence.

E. If a subpoena does not meet one of the requirements of subsection B of this section or if grounds for objection exist under rule 45 of the Arizona rules of civil procedure, a health care provider may file with the court or tribunal an objection to the inspection or copying of any or all of the records as follows:

1. On filing an objection, the health care provider shall send a copy of the objection to the patient at the patient's last known address, to the patient's attorney if known and to the party seeking the records, unless after reasonable inquiry the health care provider cannot determine the last known address of the patient.

2. On filing the objection, the health care provider has no further obligation to assert a state or federal privilege pertaining to the records or to appear or respond to a motion to compel production of records, and may produce the records if ordered by a court or tribunal. If an objection is filed, the patient or the patient's attorney is responsible for asserting or waiving any state or federal privilege that pertains to the records.

3. If an objection is filed, the party seeking production may request an order compelling production of the records. If the court or tribunal issues an order compelling production, a copy of the order shall be provided to the health care provider. On receipt of the order, the health care provider shall produce the records.

4. If applicable, an objection shall state that the health care provider is subject to the confidentiality requirements in 42 United States Code sections 290dd-3 and 290ee-3, shall state that the records may be subject to those confidentiality requirements and shall request that the court make a determination, if required under applicable federal law and regulations, on whether the submitted records are subject to discovery.

F. IF A SUBPOENA MEETS ONE OF THE REQUIREMENTS OF SUBSECTION B OF THIS SECTION, A HEALTH CARE PROVIDER MAY FILE THE MEDICAL RECORDS OR PAYMENT RECORDS UNDER SEAL PURSUANT TO SUBSECTION D OF THIS SECTION OR SHALL PRODUCE THE MEDICAL RECORDS OR PAYMENT RECORDS TO THE PARTY SEEKING THE RECORDS. IF PRODUCED TO THE PARTY SEEKING THE RECORDS, THE RECORDS SHALL BE ACCOMPANIED BY THE AFFIDAVIT OF THE CUSTODIAN OR OTHER QUALIFIED WITNESS, STATING IN SUBSTANCE THE ELEMENTS SET FORTH IN SUBSECTION D(4) OF THIS SECTION.

G. IF RECORDS PRODUCED UNDER SUBSECTION D OR SUBSECTION F OF THIS SECTION ARE ACCOMPANIED BY THE AFFIDAVIT PRESCRIBED BY SUBSECTION D(4) OF THIS SECTION, THE HEALTH CARE PROVIDER NEED NOT COMPLY WITH A NOTICE OF DEPOSITION OF THE CUSTODIAN OF RECORDS, UNLESS SO ORDERED BY A COURT OR TRIBUNAL.

F.H. If a party seeking medical records or payment records wishes to examine the original records maintained by a health care provider, the health care provider may permit the party to examine the original records if the subpoena meets one of the requirements of subsection B of this section. The party seeking the records also may petition a court or tribunal for an order directing the health care provider to allow the party to examine the original records or to file the original records under seal with the court or tribunal under subsection D of this section.

I. THIS SECTION APPLIES TO ANY PERSON OR ENTITY THAT MAINTAINS OR HANDLES MEDICAL RECORDS OR PAYMENT RECORDS, OR INFORMATION CONTAINED IN MEDICAL RECORDS OR PAYMENT RECORDS, ON BEHALF OF A HEALTH CARE PROVIDER.

6) Adult Day Health Care Facility Regulations (ADHS)

A.A.C. R9-10-511(C)

Description of Laws:

A.A.C. R9-10-511(C) requires adult day health care facilities to have medical records "recorded in ink."

Identified Barriers to Health Information Exchange:

A record "recorded in ink" presumably does not permit adult day health care facilities to use electronic health records. While the intent was undoubtedly to prohibit these facilities from keeping medical records with pencil or other non-permanent medium, the language used seems to require hand-written records.

Proposed Solution:

This regulation should be updated to permit electronic health records.

R9-10-511. Participant Records

A. The administrator shall ensure that up-to-date participant records are available to the participant or participant's representative upon 48 hours' written notice to the facility, excluding weekends and holidays.
B. Records for each participant shall include the following:
1. Full name, date of birth, social security number, and address;
2. Names, addresses, telephone numbers of participant's representative, medical provider, and other medical and nonmedical providers involved in the care of the participant;
3. Enrollment agreement;
4. Emergency information;
5. Written acknowledgment of the receipt of copies of participant rights and facility rules;
6. Signed medical provider's assessment;
7. Medical provider's orders;
8. Evidence of freedom from tuberculosis;
9. Comprehensive assessment;
10. Records of medical care and medications provided by the facility;
11. Vital signs and nutritional status;
12. Care plan;
13. Documentation of any significant changes in participant behavior or condition, including injuries and accidents, and notification of the participant's medical provider and participant's representative;
14. Signed authorization if medical information is released;
15. Determination of participant's capability of signing in or out of the facility; and
16. Discharge date, if applicable.

C. Records shall be legibly recorded ~~in ink~~. Each entry shall be dated and signed. Records shall be protected at all times from possible loss, damage, or unauthorized use.
D. Records shall be retained for three years.
E. If the facility ceases operation, copies of records shall be available upon the request of the participant or participant's representative for three years from the date of closure.

(7) Arizona Health Care Cost Containment System (AHCCCS) Regulations:

A.R.S. § 36-2901 and A.A.C. R9-22-512

Description of Laws:

Statutory and regulatory restrictions apply to disclosures by the Arizona Health Care Cost Containment System (AHCCCS) and organizations that are AHCCCS contractors, providers, and noncontracting providers.[27] The AHCCCS plan and its contractors, providers and noncontracting providers may disclose information related to AHCCCS applicants, eligible persons or members in more limited circumstances than permitted by the HIPAA Privacy Rule.[28] Significantly, the regulations require the holder of a medical record of a "former applicant, eligible person, or member" to obtain written consent from that person "before transmitting the medical record to a primary care provider."[29] On the other hand, "subcontractors are not required to obtain written consent from an eligible person or member before transmitting the eligible person's or member's medical record to a physician who: (1) provides a service to the eligible person or member under subcontract with the program contractor, (2) is retained by the subcontractor to provider services that are infrequently used or are of an unusual nature, and (3) provides a service under the contract."[30] The regulations also do not expressly permit release of AHCCCS member information for research purposes.

---

[27] A.R.S. § 36-2901 (definitions).

[28] A.A.C. R9-22-512 permits disclosures of information concerning an "eligible person, applicant, or member" only:

(1) To the individual;
(2) With authorization of the individual (where the authorization meets certain requirements);
(3) To persons or agencies for "official purposes" related to administration of the AHCCCS program. These "official purposes" include establishing eligibility and post-eligibility treatment of income; determining the amount of medical assistance; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the AHCCCS program; performing evaluations and analyses of AHCCCS operations; filing liens on property as applicable; filing claims on estates; filing, negotiating, and settling medical liens and claims; and providing services for eligible persons and members. "[P]roviding services for eligible persons and members" is read broadly to permit disclosure for "treatment, payment and health care operations," as defined under HIPAA, and to family members or friends involved in the treatment of the member;
(4) For "official purposes" related to administration of the AHCCCS program and only to the extent required in performance of duties, to employees of AHCCCS, the Social Security Administration, Arizona DES, ADHS, the federal DHHS, the Arizona Attorney General's Office, the Board of Supervisors, AHCCCS eligibility offices, and the County Attorney, as well as employees of contractors, program contractors, providers and subcontractors.
(5) To law enforcement for the purpose of an investigation, prosecution, or criminal or civil proceeding relating to the administration of the AHCCCS program, including where the member is suspected of AHCCCS fraud or abuse (and otherwise if the law enforcement official has statutory authority to obtain the information);
(6) To a review committee pursuant to A.R.S. § 36-2917; and
(7) To the extent required in the performance of duties to various government agencies.

[29] A.A.C. R9-22-512(G).

[30] A.A.C. R9-22-512(H).

Identified Barriers to Health Information Exchange:

Information about AHCCCS members will be included in HIE; indeed, AHCCCS itself is creating an HIE for AHCCCS providers. The current regulations pose the following barriers to including AHCCCS member information in an HIE:

A.A.C. R9-22-512(3) permits disclosures of information concerning an "eligible person, applicant, or member" to persons or agencies for "official purposes" related to administration of the AHCCCS program. The "official purposes" listed include "establishing eligibility and post-eligibility treatment of income; determining the amount of medical assistance; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the AHCCCS program; performing evaluations and analyses of AHCCCS operations; filing liens on property as applicable; filing claims on estates; filing, negotiating, and settling medical liens and claims; and providing services for eligible persons and members." While we believe that the phrase "providing services for eligible persons and members" is read broadly to permit disclosure for "treatment, payment and health care operations," as defined under HIPAA, and to family members or friends involved in the treatment of the member, we urge AHCCCS to consider clarifying that conclusion in its regulatory revisions.

A.A.C. R9-22-512(4) permits release of information "official purposes" related to administration of the AHCCCS program and only to the extent required in performance of duties, to employees of AHCCCS, the Social Security Administration, Arizona DES, ADHS, the federal DHHS, the Arizona Attorney General's Office, the Board of Supervisors, AHCCCS eligibility offices, and the County Attorney, as well as employees of contractors, program contractors, providers and subcontractors. We recommend that AHCCCS consider permitting release of information to ADHS and county public health officials for public health purposes.

A.A.C. R9-22-512 does not expressly permit release of AHCCCS member information for research purposes. We recommend that AHCCCS consider including this in the regulation.

To raise a broader issue, we urge AHCCCS to reconsider whether this regulation should apply to health care providers. Because health care providers are already required to follow a plethora of federal and state statutes and regulations governing the privacy of health information, we strongly AHCCCS to remove providers from the scope of this regulation.

We have not proposed suggested language, as we want to work collaboratively with AHCCCS on appropriate changes to its regulations.

Exhibit C

Coppersmith Gordon Schermer & Brockelman PLC

MEMORANDUM

DATE: September 17, 2007

TO: Arizona Health-e Connection Board of Directors

FROM: Kristen B. Rosati

RE: Arizona Health Privacy Project Phase II – Executive Summary of Proposals for Statutory and Regulatory Amendments

This fall, the Legal Working Group of the Arizona Health Privacy Project will continue its work on proposals for legislative and regulatory changes where we have identified laws that pose barriers to the implementation of e-health information exchange (HIE) in Arizona.

As you may know, we are approaching development of the statutory amendments in two phases.
Phase 1 of the legislative project includes development of proposed amendments to statutes regarding information regarding communicable disease, mental health, immunization, and genetic testing, and subpoenas for medical records. We also are proposing potential regulatory changes related to immunization, AHCCCS and adult day health are facilities regulations. Our proposals are detailed in my August 17, 2007 memorandum to the Legal Working Group, which was circulated to you earlier.

Phase 2 of the project involves the ambitious project to create a new statute governing enforcement/ penalties for inappropriate access to an HIE, and potentially crafting safe harbors for providers and other authorized individuals who access information in an HIE in an appropriate fashion. The first meeting to discuss an enforcement proposal will be **October 15, 2007.** We would benefit greatly from having representatives of your organizations participate in these discussions.

We look forward to your feedback.

Executive Summary

We are proposing that the Arizona Health-e Connection Board of Directors approve pursuing the following statutory and regulatory revisions to laws that pose barriers to the implementation of e-health information exchange (HIE) in Arizona:

(1) <u>Communicable Diseases</u>:
A.R.S. § 36-661 *et seq*., A.R.S. § 20-448.01 and A.A.C. R20-6-1204

We are proposing removing the requirement in A.R.S. § 36-663(H) that, if a disclosure of communicable disease information is made for a purpose for which an authorization is required, the disclosure must be accompanied by a statement "in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law." We believe this will not reduce any privacy protection, because where communicable disease information is disclosed to a person pursuant to a patient's authorization, the person receiving the information also must comply with the statute.[1]

We also recommend adding a provision permitting disclosure to an HIE. Because there is not a universally recognized definition for a "health information exchange," we propose to define it as an agent that conducts health information exchange, which can be broadly interpreted to fit the variety of HIEs developing. We also propose to limit the disclosure to such agents that agree to limit disclosure to those purposes permitted by the statute, so that the information has downstream protection.

We also recommend amending A.R.S. § 20-448.01and A.A.C. R20-6-1204 so that insurers may disclose HIV/AIDS in the same manner as providers. We recommend retaining those provisions essential to privacy protection, such as limitation of the type of information that may be released to an insurance medical information exchanges (which we redefine for clarity to ensure that it does not cover an HIE) and in responses to subpoenas or court orders.

Finally, we will recommend to ADHS to remove the 180-day limit on authorization found in A.A.C. R20-6-1204.

(2) <u>Mental Health Information</u>:
A.R.S. § 36-501, *et seq*.

We recommend amending the statute to permit disclosure to a third party payor or the payor's contractor for payment, case management and disease management as defined under the HIPAA Privacy Rule. We also recommend expressly permitting disclosure to an HIE.

(3) <u>Immunization Information:</u>
A.R.S. § 36-135 and A.A.C. R9-6-708

We recommend removing the prohibition against redisclosure of immunization information received from ADHS, and to provide instead that immunization information may be redisclosed as permitted by A.R.S. § 36-135 and A.A.C. R9-6-708.

---

[1] A.R.S. § 36-664(A).

This will continue to restrict who receives immunization information, but will not interfere with the exchange of immunization information for treatment and other permitted purposes.

We also recommend clarifying that disclosures to health plans are not restricted to AHCCCS and HMOs, and permitting ADHS to release immunization information directly to an HIE.

For regulatory changes, we recommend expanding the types of permissible research.

(4) Genetic Testing Information:
A.R.S. § 12-2801, *et seq*. and A.R.S. § 20-448.02, *et seq*.

We recommend that A.R.S. § 12-2801be amended to clarify that "information derived from genetic testing" was not intended to cover diagnosis of a disease or treatment for a disease. We also recommend amending A.R.S. § 12-2802 to clarify that disclosures to treating providers are permitted, and to remove the redisclosure prohibition and instead permit disclosures that otherwise are permitted under the statute. We also recommend permitting disclosures to an HIE.

Finally, we recommend amending the insurance statute, A.R.S. § 20-448.02, to permit disclosures in the same instances as A.R.S. § 12-2802. This will permit insurers to contribute genetic testing information to an HIE, as long as the HIE follows the same restrictive rules as are applicable to providers.

(5) Medical Records Subpoena Statute
A.R.S. § 12-2294.01

The current medical records subpoena statute poses three potential barriers to health care providers' participation in HIE if not clarified:

(1) Treatment of records from other sources: An increasing number of patients are presenting to hospitals and physicians with medical records from the patient's other health care providers, often stored on CDs or in other electronic form. Moreover, providers will begin to have access to information in HIE systems. The specific question presented is when records from other sources should be treated as the provider's own medical record in responding to subpoenas.

Right now, the definition of "medical records" in Arizona includes "all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers." A.R.S. § 12-2291. We believe this definition is too broad and should instead reflect the industry standard. The industry standard, as reflected in AHIMA guidance documents, treats records from other providers as not being a part of the medical record produced in response to a subpoena unless the other providers' records are used by the

responding provider in the provision of patient care. We thus propose a change in the definition of "medical record" in A.R.S. § 12-2291, to indicate that records from other sources are part of a provider's medical record only if they are used for the provision of patient care.

(2) Subpoenas issued to the HIE: The present medical records subpoena statute applies only to "health care providers" as defined above. It does not apply to HIEs or other third parties that hold medical records or payment records on behalf of health care providers. We recommend that the existing subpoena statute be extended to HIEs and others that hold records on behalf of health care providers, which would provide sufficient protection for the privacy of the health information held or managed by HIEs.

(3) Depositions of Custodians of Record: We also suggest refining the subpoena statute to clarify when health care providers and HIEs must submit their custodians of record for a deposition. Hospitals and other health care providers long have followed the practice of providing copies of subpoenaed medical records with an affidavit from the custodian of records that the copy provided is a true and complete copy. Hospitals and other providers have followed that practice so that their custodians of records do not have to be deposed to establish the admissibility of the records produced. Unfortunately, hospitals have received notices of depositions of their custodian of records, even though they provided the affidavit to establish admissibility. This is a large resource commitment—providers are required to pay their employee to attend the deposition as well as a lawyer to represent the employee in the deposition—and this resource commitment is not necessary to establish admissibility of the records. We propose a formal process to submit an affidavit in support of records produced, as well as clarify that providers are not required to submit their custodian of records for deposition if they provide a compliant affidavit.

6) <u>Adult Day Health Care Facility Regulations</u>
A.A.C. R9-10-511(C)

We recommend updating A.A.C. R9-10-511(C) to remove the requirement that adult day health care facilities to have medical records "recorded in ink."

(7) <u>Arizona Health Care Cost Containment System (AHCCCS) Regulations:</u>
A.R.S. § 36-2901 and A.A.C. R9-22-512

Working with AHCCCS, the Legal Working Group will continue to evaluate what statutory and regulatory restrictions apply to disclosures by AHCCCS and its AHCCCS contractors, providers, and noncontracting providers. These entities may disclose information related to AHCCCS applicants, eligible persons or members in more limited circumstances than permitted by the HIPAA Privacy Rule, which are outlined in our August 17 memorandum.

KBR

Exhibit D

Coppersmith Gordon Schermer & Brockelman PLC

MEMORANDUM

DATE: October 10, 2007

TO: Arizona Health-e Connection Legal Working Group

FROM: Kristen B. Rosati

RE: Arizona Health Privacy Project Phase II –
Finalizing Proposals for Statutory and Regulatory Amendments

Thank you very much for your feedback on my August 17, 2007 memorandum and its proposals for statutory and regulatory amendments. This memorandum reflects your comments to the proposed statutory and regulatory amendments.

I presented those proposals to the Arizona Health-e Connection Board of Directors on September 18, 2007. The Board decided to postpone introduction of a legislative proposal until January 2009. This will allow us to develop a more complete HIE "package" that establishes important consumer rights provisions and a more comprehensive enforcement framework, as well as remove the barriers to electronic exchange of health information within an appropriate privacy and security framework. We will have the opportunity work with stakeholders and the Arizona legislature in advance, so that we can address potential concerns to the legislative package in advance of the session.

We will be meeting in November to begin work on a new statute governing enforcement/ penalties for inappropriate access to an HIE, and potentially crafting immunity/ safe harbors for providers and other authorized individuals who access information in an HIE in an appropriate fashion. The meeting will be on **November 13, 2007, 1 p.m. to 4 p.m.** at 1700 West Washington Street, the Tower's First Floor Conference Room. Please RSVP to Kim Snyder before November 9 at ksnyder@azgita.gov or voice mail at 602-364-4795.

This is an open process, so please feel free to forward to individuals you think would be interested in these topics.

Thanks, as always, for your involvement!

1. Background

The Legal Working Group identified the following statutes and regulations as containing potential barriers to e-health data exchange in Arizona:

- Communicable disease information statutes and regulations: A.R.S. § 36-661 *et seq*., A.R.S. § 20-448.01 and A.A.C. R20-6-1204
- Mental health information statute: A.R.S. § 36-501, *et seq*.
- Immunization information: A.R.S. § 36-135 and A.A.C. R9-6-708.
- Genetic testing statutes, A.R.S. § 12-2801, *et seq*. and A.R.S. § 20-448.02, *et seq*.
- Medical record subpoena statute, A.R.S. § 12-2294.01
- AHCCCS member information regulations: A.A.C. R9-22-512
- Adult Day Health Care Facility records regulation: A.A.C. R9-10-511(C)
- Enforcement/ safe harbors

This memorandum provides background for individuals who have not been able to attend all of our meetings: it describes the laws related to sharing of the types of information identified above and the barriers we have identified in these areas. It also describes the consensus position developed at Legal Working Group meetings for proposed statutory and regulatory amendments to "fix" these barriers to e-health data exchange in Arizona.

2. Proposed Statutory Amendments for Consideration by the Arizona Health-e Connection Board of Directors

The following section provides details regarding the present laws, how those laws may constitute barriers to HIE, proposed statutory amendments, and our reasoning behind these proposals.

(1) Communicable Diseases:

A.R.S. § 36-661 *et seq*., A.R.S. § 20-448.01 and A.A.C. R20-6-1204

Description of Laws:

Arizona law requires certain health care providers and administrators of health care entities to report to the local health agency and others when they identify a case or suspected case of certain communicable diseases. In the case of HIV, AIDS, and tuberculosis, the specific reporting requirements are identified in statute.[1] In addition to these specific statutory requirements, ADHS regulations identify additional reportable communicable diseases.[2]

[1] A.R.S. § 36-621 (HIV/AIDS), A.R.S. § 36-723(D) (tuberculosis).

[2] A.A.C. R9-6-101 et seq.

Healthcare providers must preserve the confidentiality of reportable communicable disease information and may release it only for the purposes expressly listed in the statute.[3] Communicable disease information is broadly defined information and goes far beyond HIV/ AIDS information; it includes information about any "contagious, epidemic or infectious disease required to be reported to the local board of health" or ADHS that is in the possession of someone who provides health services or who obtains the information pursuant to a release (same as a "consent" or "authorization") signed by the patient.[4] At present, reportable communicable diseases include a wide variety of ailments, including flu, measles, mumps and other conditions that do not carry a stigmatizing effect.[5] Separate provisions govern when a state, county or local health department or officer may disclose communicable disease related information.[6] Given the broad scope of "communicable disease information," a HIE will certainly include communicable disease information.

Significantly, if a disclosure of communicable disease information is made for a purpose for which an authorization is required, the disclosure must be accompanied by a statement "in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law."[7] Where the information is disclosed to a person pursuant to a patient's authorization, the person receiving the information also must comply with the statute.[8]

Finally, additional restrictions in the Insurance Code apply to health plans' release of HIV/AIDS information. The insurance statute lists limited types of disclosures of

---

[3] A.R.S. § 36-664.

[4] A.R.S. § 36-661(4) and (5).

[5] See R9-6-202 (Reporting Requirements for a Health Care Provider or an Administrator of a Health Care Institution or Correctional Facility; R9-6-203 (Reporting Requirements for an Administrator of a School, Child Care Establishment, or Shelter); R9-6-204 (Clinical Laboratory Director Reporting Requirements); R9-6-205 (Reporting Requirements for a Pharmacist or Pharmacy Administrator); R9-6-206 (Local Health Agency Responsibilities Regarding Communicable Disease Reports); R9-6-207 (Federal or Tribal Entity Reporting).

[6] A.R.S. § 36-661. These persons may disclose this information only if:

(1) Specifically authorized or required by federal or state law;
(2) Made pursuant to an authorization signed by the protected person or the protected person's health care decision maker;
(3) Made to a contact of the protected person (someone who may have contracted the disease). The disclosure shall be made without identifying the protected person;
(4) For the purposes of research as authorized by state and federal law;
(5) With authorization from the director, to the national center for health statistics of the United States public health service for the purposes of conducting a search of the national death index.

[7] A.R.S. § 36-664(H).

[8] A.R.S. § 36-664(A).

HIV/AIDS information that insurers are permitted to make.[9] Like health care providers, an insurer's disclosure of HIV/AIDS-related information must be accompanied by a written statement that warns that the information is protected by state law that prohibits further disclosure of the information without the specific written consent of the person to whom it pertains or as otherwise permitted by law.[10]

Moreover, when insurers seek authorization from individuals to release HIV/AIDS information, A.A.C. R20-6-1204 places additional restrictions on those disclosures and imposes an 180-day limit on an authorization form.

Identified Barriers to Health Information Exchange:

A.R.S. § 36-664(H) and A.R.S. § 20-448.01(G) require that communicable disease or HIV/AIDS information disclosed pursuant to an authorization be accompanied by a written statement that warns the information is confidential and prohibits further disclosure without the specific written authorization of the patient or as otherwise permitted by law. This requirement for a written statement regarding re-disclosure may pose a substantial barrier to HIE. Because the definition of "communicable disease" is so broad and includes many health conditions such as flu (see discussion above), health care providers cannot segregate communicable disease information from the rest of the information in a patient's record. We thus must assume that all health information exchanged in a HIE includes communicable disease information. This will pose a barrier to HIE in the following circumstances: if an individual provides authorization to include his or her health information in the HIE (either collected by the provider or the HIE), information about that individual would need to be accompanied by a written re-disclosure warning when it was disclosed to the HIE and every time that information was disclosed by the HIE. The requirement that such notice be "written" poses obvious challenges in the electronic health information environment. But even if an electronic notice meets the written notice requirement, existing electronic health information systems cannot accommodate such a requirement.

Moreover, both A.R.S. § 36-664 and A.R.S. § 20-448.01 could be interpreted as not permitting direct disclosure of information to an HIE. Both statutes expressly list permitted disclosures, which do not include an HIE. Moreover, the insurance statute does not even permit disclosures for treatment purposes without the consent of the patient.

A.A.C. R20-6-1204 also limits an insurer's ability to release information to an HIE, as it requires a written release form for any disclosure of HIV-related information. Moreover, the 180-day limit on an authorization form would limit the ability of an HIE to handle this type of information on behalf of an insurer.

---

[9] A.R.S. § 20-448.01.

[10] A.R.S. § 20-448.01(F) and (G).

Proposed Solution:

The consensus solution developed at the June 12 meeting is to recommend removing the redisclosure notice entirely from A.R.S. § 36-664(H) and A.R.S. § 20-448.01. Both statutes already require that a person who receives communicable disease or HIV-AIDS information may not disclose that information except as authorized by the statute. Removing the written redisclosure notice thus would not reduce any privacy protection available for this type of information.

We also recommend adding a permitted disclosure to an HIE. Because there is not a universally-recognized definition for a "health information exchange,"[11] we propose to define it as an agent that conducts health information exchange. We also propose to limit the disclosure to such agents that agree to limit disclosure to those purposes permitted by the statute, so that the information is protected "downstream."

We also recommend amending A.R.S. § 20-448.01and A.A.C. R20-6-1204 so that insurers may disclose HIV/AIDS in the same manner as providers. We recommend retaining those provisions essential to privacy protection of HIV/AIDS information handled by insurers, such as limitation of the type of information that may be released to an insurance medical information exchanges (which we redefine for clarity to ensure that it does not cover an HIE) and in responses to subpoenas or court orders.

We also recommend to the ADHS to remove the 180-day limit on authorization found in A.A.C. R20-6-1204.

36-664. Confidentiality; exceptions

A. A person who obtains communicable disease related information in the course of providing a health service or obtains that information from a health care provider pursuant to an authorization shall not disclose or be compelled to disclose that information except to the following:

1. The protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker.

2. The department or a local health department for purposes of notifying a good Samaritan pursuant to subsection E of this section.

3. An agent or employee of a health facility or health care provider to provide health services to the protected person or the protected person's child or for billing or reimbursement for health services.

4. A health facility or health care provider, in relation to the procurement, processing, distributing or use of a human body or a human body part, including organs, tissues, eyes, bones, arteries, blood, semen, milk or other body fluids, for use in medical education, research or therapy or for transplantation to another person.

5. A health facility or health care provider, or an organization, committee or individual designated by the

[11] The Office of the National Coordinator for Health Information Technology, for example, defines it as "the mobilization of healthcare information electronically across organizations within a region or community," not as an entity conducting that exchange.

health facility or health care provider, that is engaged in the review of professional practices, including the review of the quality, utilization or necessity of medical care, or an accreditation or oversight review organization responsible for the review of professional practices at a health facility or by a health care provider.

6. A private entity that accredits the health facility or health care provider and with whom the health facility or health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

7. A federal, state, county or local health officer if disclosure is mandated by federal or state law.

8. A federal, state or local government agency authorized by law to receive the information. The agency is authorized to redisclose the information only pursuant to this article or as otherwise permitted by law.

9. An authorized employee or agent of a federal, state or local government agency that supervises or monitors the health care provider or health facility or administers the program under which the health service is provided. An authorized employee or agent includes only an employee or agent who, in the ordinary course of business of the government agency, has access to records relating to the care or treatment of the protected person.

10. A person, health care provider or health facility to which disclosure is ordered by a court or administrative body pursuant to section 36-665.

11. The industrial commission or parties to an industrial commission claim pursuant to section 23-908, subsection D and section 23-1043.02.

12. Insurance entities pursuant to section 20-448.01 and third party payors or the payors' contractors.

13. Any person or entity as authorized by the patient or the patient's health care decision maker.

14. A person or entity as required by federal law.

15. The legal representative of the entity holding the information in order to secure legal advice.

16. A person or entity for research only if the research is conducted pursuant to applicable federal or state laws and regulations governing research.

17. AN AGENT FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE AGENT AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO DISCLOSE COMMUNICABLE-DISEASE RELATED INFORMATION ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. At the request of the department of economic security in conjunction with the placement of children in foster care or for adoption or court-ordered placement, a health care provider shall disclose communicable disease information, including HIV-related information, to the department of economic security.

C. A state, county or local health department or officer may disclose communicable disease related information if the disclosure is any of the following:

1. Specifically authorized or required by federal or state law.

2. Made pursuant to an authorization signed by the protected person or the protected person's health care decision maker.

3. Made to a contact of the protected person. The disclosure shall be made without identifying the

protected person.

4. For the purposes of research as authorized by state and federal law.

D. The director may authorize the release of information that identifies the protected person to the national center for health statistics of the United States public health service for the purposes of conducting a search of the national death index.

E. The department or a local health department shall disclose communicable disease related information to a good Samaritan who submits a request to the department or the local health department. The request shall document the occurrence of the accident, fire or other life-threatening emergency and shall include information regarding the nature of the significant exposure risk. The department shall adopt rules that prescribe standards of significant exposure risk based on the best available medical evidence. The department shall adopt rules that establish procedures for processing requests from good Samaritans pursuant to this subsection. The rules shall provide that the disclosure to the good Samaritan shall not reveal the protected person's name and shall be accompanied by a written statement that warns the good Samaritan that the confidentiality of the information is protected by state law.

F. An authorization to release communicable disease related information shall be signed by the protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker. An authorization shall be dated and shall specify to whom disclosure is authorized, the purpose for disclosure and the time period during which the release is effective. A general authorization for the release of medical or other information, including communicable disease related information, is not an authorization for the release of HIV-related information unless the authorization specifically indicates its purpose as an authorization for the release of confidential HIV-related information and complies with the requirements of this section.

G. A person to whom communicable disease related information is disclosed pursuant to this section shall not disclose the information to another person except as authorized by this section. This subsection does not apply to the protected person or a protected person's health care decision maker.

~~H. If a disclosure of communicable disease related information is made pursuant to an authorization under subsection F of this section, the disclosure shall be accompanied by a statement in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law.~~

~~I~~H. This section does not prohibit the listing of communicable disease related information, including acquired immune deficiency syndrome, HIV-related illness or HIV infection, in a certificate of death, autopsy report or other related document that is prepared pursuant to law to document the cause of death or that is prepared to release a body to a funeral director. This section does not modify a law or rule relating to access to death certificates, autopsy reports or other related documents.

~~J~~I. If a person in possession of HIV-related information reasonably believes that an identifiable third party is at risk of HIV infection, that person may report that risk to the department. The report shall be in writing and include the name and address of the identifiable third party and the name and address of the person making the report. The department shall contact the person at risk pursuant to rules adopted by the department. The department employee making the initial contact shall have expertise in counseling persons who have been exposed to or tested positive for HIV or acquired immune deficiency syndrome.

~~K~~J. Except as otherwise provided pursuant to this article or subject to an order or search warrant issued pursuant to section 36-665, a person who receives HIV-related information in the course of providing a health service or pursuant to a release of HIV-related information shall not disclose that information to another person or legal entity or be compelled by subpoena, order, search warrant or other judicial process to disclose that information to another person or legal entity.

~~L~~K. This section and sections 36-663, 36-666, 36-667 and 36-668 do not apply to persons or entities subject to regulation under title 20.

20-448.01. Required insurance procedures relating to HIV information; confidentiality; violations; penalties; definitions

A. In this section unless the context otherwise requires:

1. "Confidential HIV-related information" means information concerning whether a person has had an HIV-related test or has HIV infection, HIV-related illness or acquired immune deficiency syndrome and includes information which identifies or reasonably permits identification of that person or the person's contacts.

2. "HIV" means the human immunodeficiency virus.

3. "HIV-related test" means a laboratory test or series of tests for the virus, components of the virus or antibodies to the virus thought to indicate the presence of HIV infection.

4. "Protected person" means a person who takes an HIV-related test or who has been diagnosed as having HIV infection, acquired immune deficiency syndrome or HIV-related illness.

5. "Person" includes all entities subject to regulation under title 20, the employees, contractors and agents thereof, and anyone performing insurance related tasks for such entities, employees, contractors or agents.

B. Except as otherwise specifically authorized or required by this state or by federal law, no person may require the performance of, or perform an HIV-related test without first receiving the specific written informed consent of the subject of the test who has capacity to consent or, if the subject lacks capacity to consent, of a person authorized pursuant to law to consent for that person. Written consent shall be in a form as prescribed by the director.

C. No person who obtains confidential HIV-related information in the course of processing insurance information or insurance applications or pursuant to a release of confidential HIV-related information may disclose or be compelled to disclose that information except AS PERMITTED IN SECTION 36-664, EXCEPT THAT IN A DISCLOSURE OF INFORMATION TO A CONSUMER REPORTING AGENCY OR OTHER ORGANIZATION WHOSE PURPOSE IS TO DETECT FRAUD IN INSURANCE, SUCH AS THE MEDICAL INFORMATION BUREAU: ~~to the following:~~

~~1. The protected person or, if the protected person lacks capacity to consent, a person authorized pursuant to law to consent for the protected person.~~

~~2. A person to whom disclosure is authorized in writing pursuant to a release as set forth in subsection E of this section, including but not limited to a physician designated by the insured or a medical information exchange for insurers operated under procedures intended to ensure confidentiality, provided that1.~~

~~1. In the case of a medical information exchang~~e:

~~(a)~~ 1. The insurer will not report that blood tests of an applicant showed the presence of the AIDS virus antibodies, but only that unspecified blood test results were abnormal.

~~(b)~~ 2. Reports must use a general code that also covers results of tests for many diseases or conditions, such as abnormal blood counts that are not related to HIV, AIDS, AIDS related complex or similar diseases.

~~3. A government agency specifically authorized by law to receive the information. The agency is~~

~~authorized to redisclose the information only pursuant to this section or as otherwise permitted by law.~~

~~42. A person regulated by this title to which disclosure is ordered by a court or administrative body ONLY pursuant to section 36-665.~~

~~5. The industrial commission or parties to an industrial commission claim pursuant to the provisions of section 23-908, subsection D and section 23-1043.02.~~

D. Test results and application responses may be shared with the underwriting departments of the insurer and reinsurers, or to those contractually retained medical personnel, laboratories, and insurance affiliates, excluding agents and brokers, which are involved in underwriting decisions regarding the individual's application if disclosure is reasonably necessary to make the underwriting decision regarding such application, and claims information may be shared with claims personnel and attorneys reviewing claims if disclosure is reasonably necessary to process and resolve claims.

~~E. A release of confidential HIV-related information pursuant to subsection C, paragraph 2 of this section shall be signed by the protected person or, if the protected person lacks capacity to consent, a person authorized pursuant to law to consent for the protected person. A release shall be dated and shall specify to whom disclosure is authorized, the purpose for disclosure and the time period during which the release is effective. A general authorization for the release of medical or other information is not a release of confidential HIV-related information unless the authorization specifically indicates its purpose as a general authorization and an authorization for the release of confidential HIV-related information and complies with the requirements of this section.~~

~~F~~E. A person to whom confidential HIV-related information is disclosed pursuant to this section shall not disclose the information to another person except as authorized by this section. This subsection does not apply to the protected person or a person who is authorized pursuant to law to consent for the protected person.

~~G. If a disclosure of confidential HIV-related information is made pursuant to the provisions of a written release as permitted by subsection C, paragraph 2 of this section, the disclosure shall be accompanied by a statement in writing which warns that the information is from confidential records which are protected by state law that prohibits further disclosure of the information without the specific written consent of the person to whom it pertains or as otherwise permitted by law.~~

~~H. The person making a disclosure in accordance with subsection C, paragraphs 3, 4 and 5, and subsection G of this section shall keep a record of all disclosures for the time period prescribed by the director. On request, a protected person or his legal representative shall have access to the record.~~

~~I~~.F. Except as otherwise provided pursuant to this section or subject to an order or search warrant issued pursuant to section 36-665, no person who receives confidential HIV-related information pursuant to a release of confidential HIV-related information may disclose that information to another person or legal entity or be compelled by subpoena, order, search warrant or other judicial process to disclose that information to another person or legal entity.

~~J~~G. The director shall adopt rules to implement the allowable tests and testing procedures, written consent to perform a human immunodeficiency virus relate test, procedures for confidentiality and disclosure of medical information and procedures for gathering underwriting information and may adopt additional rules reasonable and necessary to implement this section.

~~K~~H. Notwithstanding any other provision of law to the contrary, nothing in this section shall be interpreted to restrict the director's authority to full access to records of any entity subject to regulation under title 20, including but not limited to all records containing confidential HIV-related information. The director may only redisclose confidential HIV-related information in accordance with this section.

~~L~~I. A protected person, whose rights provided in this section have been violated by a person or entity

described in subsection A, paragraph 5 of this section, has those individual remedies specified in section 20-2118 against such a person or entity.

R20-6-1204. Release of Confidential HIV-related Information; Release Form

A. ~~Except as required by law or authorized pursuant to a written consent to be tested, a~~An insurer shall ~~not~~ disclose confidential HIV-related information ONLY AS PERMITTED BY ARIZONA REVISED STATUTES SECTION 20-448.01~~01to any person unless a written release form is executed by the applicant or, if the applicant lacks legal capacity to consent to such release, by a person authorized by law to consent to the release of information on behalf of the applicant. The applicant or the applicant's legal representative shall be entitled to receive a copy of the release. A photocopy shall be as valid as the original~~.

B. The applicant or the applicant's legal representative shall be entitled to receive a copy of the release FOR CONFIDENTIAL HIV-RELATED INFORMATION. A photocopy shall be as valid as the original. Such written release form shall contain the following information:
1. The name and address of the person to whom the information shall be disclosed;
2. The specific purpose for which disclosure is to be made; and
~~3. The time period during which the written release is to be effective but in no case shall such time period exceed 180 days from the date the release is signed by the applicant or the applicant's legal representative;~~
~~4~~3. The signature of the applicant or of the person authorized by law to consent to such release, and the date the release form was signed.

(2) Mental Health Information:

A.R.S. § 36-501, *et seq*.

Description of Laws:

The Arizona mental health statutes have special restrictions on the disclosure of mental health information.[12] These statutes have limited applicability, however, and apply only to mental health providers and health care institutions licensed as behavioral health providers, including those providing inpatient and outpatient mental health services.[13] A "mental health provider" includes physicians and other providers of mental health or behavioral health services who are involved in evaluating, caring for, treating or rehabilitating a patient.[14] Health care providers that provide mental or behavioral health services but who are not licensed as behavioral health providers, such as hospital emergency departments that provide psychiatric consultations, are not subject to Arizona mental health statutes and regulations.

Information contained in mental health records is confidential and may be released only as expressly permitted by the statute.[15] (The HIPAA Privacy Rule also contains

[12] A.R.S. § 36-501 et seq.

[13] A.R.S. § 36-501(19).

[14] A.R.S. § 36-501(27).

[15] A.R.S. § 36-509

additional restrictions on the use and disclosure of "psychotherapy notes"—the mental health care professional's personal notes kept separate from the regular medical record.[16])

Identified Barriers to Health Information Exchange:

A.R.S. § 36-509(14) permits disclosure to a "third party payor or the payor's contractor to obtain reimbursement for health care, mental health care or behavioral health care provided to the patient." The consensus position developed at the June 12 meeting is that this is not broad enough to facilitate the use of information in the HIE for such purposes as utilization review, medical necessity determinations, case management, disease management, and other treatment-related functions that are necessary for behavioral health care.

Moreover, A.R.S. § 36-509 could be interpreted as not permitting direct disclosure of information to an HIE; the statute expressly lists permitted disclosures, which do not include an HIE.

Proposed Solution:

We recommend amending the statute to permit disclosure to third party payors or the payor's contractor for payment, case management, and disease management as defined under the HIPAA Privacy Rule. We also recommend expressly permitting disclosure to an HIE.

36-509. Confidential records

A. A health care entity must keep records and information contained in records confidential and not as public records, except as provided in this section. Records and information contained in records may only be disclosed to:

1. Physicians and providers of health, mental health or social and welfare services involved in caring for, treating or rehabilitating the patient.

2. Individuals to whom the patient or the patient's health care decision maker has given authorization to have information disclosed.

3. Persons authorized by a court order.

4. Persons doing research only if the activity is conducted pursuant to applicable federal or state laws and regulations governing research.

5. The state department of corrections in cases in which prisoners confined to the state prison are patients in the state hospital on authorized transfers either by voluntary admission or by order of the court.

6. Governmental or law enforcement agencies if necessary to:

[16] 45 C.F.R. § 164.501.

(a) Secure the return of a patient who is on unauthorized absence from any agency where the patient was undergoing evaluation and treatment.

(b) Report a crime on the premises.

(c) Avert a serious and imminent threat to an individual or the public.

7. Persons, including family members, actively participating in the patient's care, treatment or supervision. A health care provider may only release information relating to the patient's diagnosis, prognosis, need for hospitalization, anticipated length of stay, discharge plan, medication, medication side effects and short-term and long-term treatment goals. A health care provider may make this release only after the treating professional or that person's designee interviews the patient or the patient's health care decision maker and the patient or the patient's health care decision maker does not object, unless federal or state law permits the disclosure. If the patient does not have the opportunity to object to the disclosure because of incapacity or an emergency circumstance and the patient's health care decision maker is not available to object to the release, the health care provider in the exercise of professional judgment may determine if the disclosure is in the best interests of the patient and, if so, may release the information authorized pursuant to this paragraph. A decision to release or withhold information is subject to review pursuant to section 36-517.01. The health care provider must record the name of any person to whom any information is given under this paragraph.

8. A state agency that licenses health professionals pursuant to title 32, chapter 13, 15, 17, 19.1 or 33 and that requires these records in the course of investigating complaints of professional negligence, incompetence or lack of clinical judgment.

9. A state or federal agency that licenses health care providers.

10. A governmental agency or a competent professional, as defined in section 36-3701, in order to comply with chapter 37 of this title.

11. Human rights committees established pursuant to title 41, chapter 35. Any information released pursuant to this paragraph shall comply with the requirements of section 41-3804 and applicable federal law and shall be released without personally identifiable information unless the personally identifiable information is required for the official purposes of the human rights committee. Case information received by a human rights committee shall be maintained as confidential. For the purposes of this paragraph, "personally identifiable information" includes a person's name, address, date of birth, social security number, tribal enrollment number, telephone or telefacsimile number, driver license number, places of employment, school identification number and military identification number or any other distinguishing characteristic that tends to identify a particular person.

12. A patient or the patient's health care decision maker pursuant to section 36-507.

13. The department of public safety by the court to comply with the requirements of section 36-540, subsection N.

14. A third party payor or the payor's contractor FOR PAYMENT, CASE MANAGEMENT AND DISEASE MANAGEMENT PURPOSES, AS DEFINED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 160 AND PART 164, SUBPART E)~~to obtain reimbursement for health care, mental health care or behavioral health care provided to the patient~~.

15. A private entity that accredits the health care provider and with whom the health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

16. The legal representative of a health care entity in possession of the record for the purpose of securing

legal advice.

17. A person or entity as otherwise required by state or federal law.

18. A person or entity as permitted by the federal regulations on alcohol and drug abuse treatment (42 Code of Federal Regulations part 2).

19. A person or entity to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

20. A person maintaining health statistics for public health purposes as authorized by law.

21. A grand jury as directed by subpoena.

22. AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO DISCLOSE RECORDS AND INFORMATION CONTAINED IN RECORDS ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. Information and records obtained in the course of evaluation, examination or treatment and submitted in any court proceeding pursuant to this chapter or title 14, chapter 5 are confidential and are not public records unless the hearing requirements of this chapter or title 14, chapter 5 require a different procedure. Information and records that are obtained pursuant to this section and submitted in a court proceeding pursuant to title 14, chapter 5 and that are not clearly identified by the parties as confidential and segregated from nonconfidential information and records are considered public records.

C. Notwithstanding subsections A and B of this section, the legal representative of a patient who is the subject of a proceeding conducted pursuant to this chapter and title 14, chapter 5 has access to the patient's information and records in the possession of a health care entity or filed with the court.

(3) Immunization Information:

A.R.S. § 36-135 and A.A.C. R9-6-708

Description of Laws:

A.R.S. § 36-135 and A.A.C. R9-6-708 restrict the purposes for which ADHS may release immunization data. Specifically, A.R.S. § 36-135(D) permits ADHS to release identifying information contained in immunization data "only to the child's health care professional, parent, guardian, health care service organization, the Arizona health care cost containment system and its providers as defined in title 36, chapter 29, or a school official who is authorized by law to receive and record immunization records."[17] ADHS also "may, by rule, release immunization information to persons for a specified purpose."[18]

A.A.C. R9-6-708 additionally permits ADHS to release immunization information to:

[17] A.R.S. § 36-135(D).

[18] Id.

(1) an authorized representative of a state or local health agency for the control, investigation, analysis, or follow-up of disease; (2) a child care administrator, to determine the immunization status of a child in the child care; (3) an authorized representative of WIC, to determine the immunization status of a child enrolled in WIC; (4) an individual or organization authorized by the Department, to conduct medical research to evaluate medical services and health related services, health quality, immunization data quality, and efficacy; or (5) an authorized representative of an out-of-state agency, including a state health department, local health agency, school, child care, health care provider, or a state agency that has legal custody of a child.

A.R.S. § 36-135(E) additionally specifies that information in the ADHS immunization data system is confidential and that "a person who is authorized to receive confidential information under subsection D shall not disclose this information to any other person" Substantial penalties are in place for violating these confidentiality provision: (1) "A health care professional who does not comply with the requirements of this section violates a law or task applicable to the practice of medicine and an act of unprofessional conduct";[19] and (2) "any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor."[20]

Identified Barriers to Health Information Exchange:

Many physicians believe it would be useful to have immunization information in an HIE, as patients often do not recall or retain this information in their records. If an HIE will be populated with immunization data from ADHS, rather than directly from health care providers, the immunization statute and ADHS regulations may pose the following barriers to including this information in the HIE.

First, and most significantly, the statute specifies that "a person who is authorized to receive confidential information under subsection D shall not disclose this information to any other person." This provision would prohibit HIEs from handling immunization information received from ADHS, despite the value immunization information has for patient care. This provision would also prohibit providers from releasing immunization information to an HIE if the providers received that information from ADHS.

Second, A.R.S. § 36-135 and A.A.C. R9-6-708 permit release of information to AHCCCS and "health care services organizations" (HMOs), but not other insurers. While Arizona HIEs have not determined yet whether and when insurers will have access to information in an HIE, this provision's distinction between HMOs and other insurers may interfere with the participation of some insurers in valuable exchange efforts.

Next, to the extent that information handled by an HIE will be utilized for research purposes (of course, only with approval by an Institutional Review Board and pursuant

[19] A.R.S. § 36-135(G).

[20] A.R.S. § 36-135(H).

to all applicable federal regulations governing human subject research), the regulations permit ADHS to release information only for health services research, not other types of research.

Finally, A.R.S. § 36-135 would not permit ADHS to release immunization information directly to an HIE.

3. Proposed Solution:

The consensus at the June 12 meeting was to remove the absolute prohibition against redisclosure of immunization information, and instead to provide that immunization information may be redisclosed as permitted by A.R.S. § 36-135 and A.A.C. R9-6-708. This will continue to restrict who receives immunization information, but will not interfere with the exchange of immunization information for treatment and other permitted purposes.

We also recommend clarifying that disclosures to health plans are not restricted to AHCCCS and HMOs, and permitting ADHS to release immunization information directly to an HIE.

For regulatory changes, we recommend expanding the types of permissible research.

36-135. Child immunization reporting system; requirements; access; confidentiality; immunity; violation; classification

A. The child immunization reporting system is established in the department to collect, store, analyze, release and report immunization data.

B. Beginning on January 1, 1998, a health care professional who is licensed under title 32 to provide immunizations shall, except as provided in subsection I, report the following information:

1. The health care professional's name, business address and business telephone number.

2. The child's name, address, the child's social security number if known and not confidential, gender, date of birth and mother's maiden name.

3. The type of vaccine administered and the date it is administered.

C. The health care professional may submit this information to the department on a weekly or monthly basis by telephone, facsimile, mail, computer or any other method prescribed by the department.

D. Except as provided in subsection I, the department shall release identifying information only to the child's health care professional, parent, guardian, AN ENTITY REGULATED UNDER TITLE 20 ~~health care service organization~~, the Arizona health care cost containment system and its providers as defined in title 36, chapter 29, ~~or~~ a school official who is authorized by law to receive and record immunization records, OR AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF IDENTIFYING INFORMATION AND TO DISCLOSE IDENTIFYING INFORMATION ONLY FOR THE PURPOSES PERMITTED IN THIS SECTION. The department may, by rule, release immunization information to persons for a specified purpose. The department may release nonidentifying summary statistics.

E. Identifying information in the system is confidential. A person who is authorized to receive confidential

information under subsection D OR DEPARTMENT RULE shall ~~not~~ disclose this information ~~to any other person~~ ONLY AS PERMITTED BY THIS SECTION OR DEPARTMENT RULE.

F. A health care professional who provides information in good faith pursuant to this section is not subject to civil or criminal liability.

G. A health care professional who does not comply with the requirements of this section violates a law or task applicable to the practice of medicine and an act of unprofessional conduct.

H. Any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor.

I. At the request of the child's parent or guardian, the department of health services shall provide a form to be signed that allows confidential immunization information to be withheld from all persons including persons authorized to receive confidential information pursuant to subsection D. If the request is delivered to the health care professional prior to the immunization, the health care professional shall not forward the information required under subsection B to the department.

(4) Genetic Testing Information:

A.R.S. § 12-2801, *et seq*. and A.R.S. § 20-448.02, *et seq*.

Description of the Laws:

Arizona law contains significant restrictions on disclosure of genetic testing and information derived from genetic testing, due to the heightened concern with the potential for discrimination in employment and insurance if information related to genetic predisposition to disease is released. On the other hand, genetic testing information is becoming increasingly significant information for diagnosis and effective treatment as the industry develops "personalized medicine"; information about the genetics of a particular cancer tumor or the ability to metabolize warfarin, for example, may make a significant difference in what treatment is provided to a particular patient.

A.R.S. § 12-2801, *et seq*., protects "genetic testing and information derived from genetic testing." Genetic testing includes "a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies, including carrier status, that: (i) Are linked to physical or mental disorders or impairments; (ii) Indicate a susceptibility to any illness, disease, impairment or other disorder, whether physical or mental; or (iii) Demonstrate genetic or chromosomal damage due to any environmental factor."[21] The phrase "information derived from genetic testing" is not defined.

[21] Id. Genetic testing does not include: "(i) Chemical, blood and urine analyses that are widely accepted and used in clinical practice and that are not used to determine genetic traits; (ii) Tests used in a criminal investigation or prosecution or as a result of a criminal conviction; (iii) Tests for the presence of the human immunodeficiency virus; (iv) Tests to determine paternity conducted pursuant to title 25, chapter 6, article 1; or (v) Tests given for use in biomedical research that is conducted to generate scientific knowledge about genes or to learn about the genetic basis of disease or for developing pharmaceutical and other treatment of disease." A.R.S. § 12-2801.

The statute permits disclosure without authorization only to the patient and the patient's health care decision maker, the patient's health care provider, researchers (if federal confidentiality requirements are followed), organ procurement agencies and the state registries, and permits limited internal uses by the provider.[22] In addition, the statute prohibits a person holding genetic testing and information derived from genetic testing from producing that information pursuant to a subpoena in a manner that allows identification of the person tested, unless the disclosure otherwise falls within the eleven permitted uses and disclosures listed in the statute.[23] Importantly, the statute applies to any person who receives genetic testing information: "[A] person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person."[24]

Health care organizations that are subject to regulation by the Arizona Department of Insurance also must comply with A.R.S. § 20-448.02. This statute requires an insurance company to obtain written informed consent for genetic testing, and prohibits release of the genetic testing results to anyone without the express consent of the person tested.[25] (A.R.S. § 12-2802 provides that it does not affect the title 20 provisions governing insurance entities' handling of genetic testing information.)

Identified Legal Barriers to Health Information Exchange**:**

The phrase "information derived from genetic testing" in A.R.S. § 12-2801 is not defined; an individual involved in drafting the statute has explained that this phrase was intended to cover genetic testing results and reports of those results, but not diagnosis of a disease or treatment for a disease. Indeed, if "information derived from genetic testing" were to include the diagnosis of a genetically-based disease or treatment for such a disease, it would be exceedingly difficult for providers to segregate that information from the rest of the record. Difficulty in segregating information would have the effect of preventing providers from engaging in HIE.

We also noted confusion about when disclosures are permitted to health care providers. A.R.S. § 12-2802(6) permits disclosure to an agent or employee of a health care provider only if: (a) The health care provider performs the test or is authorized to obtain the test results by the person tested for the purposes of genetic counseling or treatment; (b) The agent or employee provides patient care, treatment or counseling; and (c) The agent or employee needs to know the information in order to conduct the test or provide patient care, treatment or counseling. On the other hand, subsection (11) permits disclosures to a "health care provider that assumes the responsibility to provide care for, or

---

22 See A.R.S. § 12-2802(A).

23 A.R.S. § 12-2802(B) – (C).

24 A.R.S. § 12-2802(F).

25 A genetic test in the insurance statute is similarly defined as "an analysis of an individual's DNA, gene products or chromosomes that indicates a propensity for or susceptibility to illness, disease, impairment or other disorders, whether physical or mental, or that demonstrates genetic or chromosomal damage due to environmental factors, or carrier status for disease or disorder." A.R.S. § 20-448.02.

consultation to, the patient from another health care provider that had access to the patient's genetic records"—in other words, to a treating provider (without the restrictions set forth in subsection (6). Confusion about when disclosures to treating providers are permitted may interfere with HIE.

A.R.S. § 12-2802(F) applies to any person who receives genetic testing, and provides that "a person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person." This phrase would prevent providers who receive genetic testing information from releasing it to an HIE or directly to other providers for treatment purposes.

Finally, A.R.S. § 20-448.02 requires an insurance company from releasing genetic testing results to anyone without the express consent of the person tested, including to a treating provider or to an HIE.

Proposed Solution:

We recommend that A.R.S. § 12-2801 be amended to clarify that "information derived from genetic testing" was not intended to cover diagnosis of a disease or treatment for a disease. We also recommend amending A.R.S. § 12-2802 to clarify that disclosure to treating providers are permitted, and to remove the redisclosure prohibition and instead permit disclosures that otherwise are permitted under the statute. We also recommend adding disclosures to an HIE as a permissible disclosure.

Finally, we recommend amending the insurance statute, A.R.S. § 20-448.02, to permit disclosures in the same instances as A.R.S. § 12-2802. This will permit insurers to contribute this information to an HIE, as well.

12-2801. Definitions

In this chapter, unless the context otherwise requires:

1. "Genetic test" or "genetic testing":

(a) Means a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies, including carrier status, that:

(i) Are linked to physical or mental disorders or impairments.

(ii) Indicate a susceptibility to any illness, disease, impairment or other disorder, whether physical or mental.

(iii) Demonstrate genetic or chromosomal damage due to any environmental factor.

(b) Does not include:

(i) Chemical, blood and urine analyses that are widely accepted and used in clinical practice and that are not used to determine genetic traits.

(ii) Tests used in a criminal investigation or prosecution or as a result of a criminal conviction.

(iii) Tests for the presence of the human immunodeficiency virus.

(iv) Tests to determine paternity conducted pursuant to title 25, chapter 6, article 1.

(v) Tests given for use in biomedical research that is conducted to generate scientific knowledge about genes or to learn about the genetic basis of disease or for developing pharmaceutical and other treatment of disease.

2. "Health care decision maker" means a person who is authorized to make health care treatment decisions for the patient, including a parent of a minor and a person who is authorized to make these decisions pursuant to title 14, chapter 5, article 2 or 3 or section 8-514.05, 36-3221, 36-3231 or 36-3281.

3. "Health care provider" means physicians licensed pursuant to title 32, chapter 13 or 17, physician assistants licensed pursuant to title 32, chapter 25, registered nurse practitioners licensed pursuant to title 32, chapter 15, health care institutions as defined in section 36-401 and clinical laboratories licensed pursuant to title 36, chapter 4.1.

4. "INFORMATION DERIVED FROM GENETIC TESTING" IS INFORMATION ABOUT THE RESULTS OF A GENETIC TEST AND DOES NOT INCLUDE INFORMATION REFLECTING A DIAGNOSIS OF OR TREATMENT FOR A DISEASE.

12-2802. Confidentiality of genetic testing results; disclosure

A. Except as otherwise provided in this article, genetic testing and information derived from genetic testing are confidential and considered privileged to the person tested and shall be released only to:

1. The person tested.

2. Any person who is specifically authorized in writing by the person tested or by that person's health care decision maker to receive this information.

3. The health care decision maker of the person tested.

4. A researcher for medical research or public health purposes only if the research is conducted pursuant to applicable federal or state laws and regulations governing clinical and biological research or if the identity of the individual providing the sample is not disclosed to the person collecting and conducting the research.

5. A third person if approved by a human subjects review committee or a human ethics committee, with respect to persons who are subject to an Arizona cancer registry OR OTHER DISEASE REGISTRY.

~~6. An authorized agent or employee of a health care provider if all of the following are true:~~

~~(a) The health care provider performs the test or is authorized to obtain the test results by the person tested for the purposes of genetic counseling or treatment.~~

~~(b) The agent or employee provides patient care, treatment or counseling.~~

~~(c) The agent or employee needs to know the information in order to conduct the test or provide patient care, treatment or counseling.~~

~~7~~6. A health care provider that procures, processes, distributes or uses:

(a) A human body part from a deceased person with respect to medical information regarding that person.

(b) Semen or ova for the purpose of artificial insemination.

~~8~~7. A health care provider to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

~~9~~8. The authorized agent of a federal, state or county health department to conduct activities specifically authorized pursuant to the laws of this state for the birth defects registry, children's rehabilitative services, newborn screening and sickle cell diagnosis and treatment programs and chronic, environmentally provoked and infectious disease programs.

~~10~~9. To obtain legal advice, the legal representative of a health care provider that is in possession of the medical record.

~~11~~10. A health care provider that assumes the responsibility to provide care for, or consultation to, the patient ~~from another health care provider that had access to the patient's genetic records~~.

11. AN ENTITY FOR THE PURPOSES OF HEALTH INFORMATION EXCHANGE, IF THE ENTITY AGREES TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AND TO ONLY DISCLOSE GENETIC TESTING AND INFORMATION DERIVED FROM GENETIC TESTING FOR THE PURPOSES PERMITTED IN THIS SECTION.

B. A person shall not disclose or be compelled to disclose the identity of any person on whom a genetic test is performed or the results of a genetic test in a manner that allows identification of the person tested except to the persons specified in the circumstances set forth in subsection A of this section.

C. If genetic testing information is subpoenaed, a health care provider shall respond pursuant to section 12-2294.01, subsection E. In determining whether to order production of the genetic testing information, the court shall take all steps necessary to prevent the disclosure or dissemination of that information.

D. Except as provided in this section, chapter 13, article 7.1 of this title does not apply to GENETIC TESTING OR INFORMATION DERIVED FROM genetic testing ~~information~~ that is contained within a patient's medical record.

E. Following the death of a person who had genetic testing performed, the release of the testing information is governed by section 12-2294, subsection D, except that the person may deny, release or limit release of the genetic testing results by adopting a provision in a testamentary document.

F. Except as specifically provided in this article, a person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person EXCEPT AS PROVIDED IN THIS SECTION.

G. A health care provider and the provider's agents and employees that act in good faith and that comply with this article are not subject to civil liability. The good faith of a health care provider that complies with this article is presumed. The presumption may be rebutted by a preponderance of the evidence.

H. This article does not limit the effect of title 20 provisions governing the confidentiality and use of genetic testing information.

20-448.02. Genetic testing; informed consent; definitions

A. Except as otherwise specifically authorized or required by this state or by federal law, a person shall not require the performance of or perform a genetic test without first receiving the specific written informed consent of the subject of the test who has the capacity to consent or, if the person subject to the test lacks the capacity to consent, of a person authorized pursuant to law to consent for that person. Written consent shall be in a form as prescribed by the director. The results of a genetic test performed pursuant

to this subsection are privileged and confidential and may not be released to any party, ~~without the expressed consent of the subject of the test~~. EXCEPT AS PERMITTED IN ARIZONA REVISED STATUTES, SECTION 12-2802.

B. As used in this section:

1. "Gene products" means gene fragments, nucleic acids or proteins derived from deoxyribonucleic acids that would be a reflection of or indicate DNA sequence information.

2. "Genetic test" means an analysis of an individual's DNA, gene products or chromosomes that indicates a propensity for or susceptibility to illness, disease, impairment or other disorders, whether physical or mental, or that demonstrates genetic or chromosomal damage due to environmental factors, or carrier status for disease or disorder.

(5) Medical Records Subpoena Statute

A.R.S. § 12-2294.01

Description of Laws:

The medical records subpoena statute, A.R.S. § 12-2294.01, governs how "health care providers" may produce medical records and payment records in response to subpoenas. "Health care providers" include licensed health care professionals that maintain medical records, health care institutions, ambulance services, and HMOs. The statute generally requires a patient to sign an authorization before releasing medical or payment records pursuant to a subpoena, but there are various exceptions in the statute. (See below.)

Identified Barriers to Health Information Exchange:

The current medical records subpoena statute poses three potential barriers to health care providers' participation in HIE if not clarified: (1) how do providers' handle other providers' records and HIE records in their responses to subpoenas; (2) how are subpoenas issued to an HIE *itself* handled; and (3) how are depositions of record custodians handled?

(1) Treatment of records from other sources: An increasing number of patients are presenting to hospitals and physicians with medical records from the patient's other health care providers, often stored on CDs or in other electronic form. Moreover, providers will begin to have access to information in HIE systems. The specific question presented is when records from other sources should be treated as the provider's own medical record in responding to subpoenas.

Right now, the definition of "medical records" in Arizona includes "all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers." A.R.S. § 12-2291. We believe this definition is too broad and should instead reflect the industry standard. The industry standard, as reflected in AHIMA guidance

documents, treats records from other providers as not being a part of the medical record produced in response to a subpoena unless the other providers' records are used by the responding provider in the provision of patient care.[26]

(2) Subpoenas issued to the HIE: The present medical records subpoena statute applies only to "health care providers" as defined above. It does not apply to HIEs or other third parties that hold medical records or payment records on behalf of health care providers. This may pose a barrier to health care providers' participation in an HIE—some may be wary of entrusting their patients' health information to an HIE unless the HIE has the same protections as the health care providers in responding to a subpoena.

(3) Depositions of Custodians of Record: We also suggest refining the subpoena statute to clarify when health care providers and HIEs must submit their custodians of record for a deposition. Hospitals and other health care providers long have followed the practice of providing copies of subpoenaed medical records with an affidavit from the custodian of records that the copy provided is a true and complete copy. Hospitals and other providers have followed that practice so that their custodians of records do not have to be deposed to establish the admissibility of the records produced. Unfortunately, hospitals have received notices of depositions of their custodian of records, even though they provided the affidavit to establish admissibility. This is a large resource commitment—providers are required to pay their employee to attend the deposition as well as a lawyer to represent the employee in the deposition—and this resource commitment is not necessary to establish admissibility of the records. This will be an equally large, and unnecessary, resource commitment for developing HIEs, as well.

Proposed Solutions:

First, to deal with the treatment of medical records from other sources, the Legal Working Group proposes a change in the definition of "medical record" in A.R.S. § 12-2291, to indicate that records from other sources are part of a provider's medical record only if they are used for the provision of patient care. This new language would reflect the national standard that records received from other sources (whether other health care providers, an HIE, or the patient's personal health record), would only be a part of the provider's own medical record if the provider uses those records to provide care to the patient.

Second, we recommend that the existing subpoena statute be extended to HIEs and others that hold records on behalf of health care providers, which would provide sufficient protection for the privacy of the health information held or managed by HIEs. We favor extending the statute to any third parties that hold or manage health information on behalf of health care providers, as this would also provide protection for vendors other than HIEs that hold or manage health information on behalf of health care providers.

---

[26] Id.

Third, we propose a formal process to submit an affidavit in support of records produced, as well as clarify that providers are not required to submit their custodian of records for deposition if they provide a compliant affidavit.

12-2291. Definitions

In this article, unless the context otherwise requires:

1. "Contractor" means an agency or service that duplicates medical records on behalf of health care providers.

2. "Department" means the department of health services.

3. "Health care decision maker" means an individual who is authorized to make health care treatment decisions for the patient, including a parent of a minor or an individual who is authorized pursuant to section 8-514.05, title 14, chapter 5, article 2 or 3 or section 36-3221, 36-3231 or 36-3281.

4. "Health care provider" means:

(a) A person who is licensed pursuant to title 32 and who maintains medical records.

(b) A health care institution as defined in section 36-401.

(c) An ambulance service as defined in section 36-2201.

(d) A health care services organization licensed pursuant to title 20, chapter 4, article 9.

5. "Medical records" means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment BY THE HEALTH CARE PROVIDER, including medical records that are prepared by a health care provider or RECEIVED FROM ~~by~~ other providers THAT ARE USED IN THE PROVISION OF PATIENT CARE BY THE HEALTH CARE PROVIDER. Medical records do not include materials that are prepared in connection with utilization review, peer review or quality assurance activities, including records that a health care provider prepares pursuant to section 36-441, 36-445, 36-2402 or 36-2917. Medical records do not include recorded telephone and radio calls to and from a publicly operated emergency dispatch office relating to requests for emergency services or reports of suspected criminal activity, but shall include communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the diagnosis or treatment of a person.

6. "Payment records" means all communications related to payment for a patient's health care that contain individually identifiable information.

7. "Source data" means information that is summarized, interpreted or reported in the medical record, including x-rays and other diagnostic images.

12-2294.01. Release of medical records or payment records to third parties pursuant to subpoena

A. A subpoena seeking medical records or payment records shall be served on the health care provider and any party to the proceedings at least ten days before the production date on the subpoena.

B. A subpoena that seeks medical records or payments records must meet one of the following

requirements:

1. The subpoena is accompanied by a written authorization signed by the patient or the patient's health care decision maker.

2. The subpoena is accompanied by a court or tribunal order that requires the release of the records to the party seeking the records or that meets the requirements for a qualified protective order under the health insurance portability and accountability act privacy standards (42 Code of Federal Regulations section 164.512(e)).

3. The subpoena is a grand jury subpoena issued in a criminal investigation.

4. The subpoena is issued by a health profession regulatory board as defined in section 32-3201.

5. The health care provider is required by another law to release the records to the party seeking the records.

C. If a subpoena does not meet one of the requirements of subsection B of this section, a health care provider shall not produce the medical records or payment records to the party seeking the records, but may either file the records under seal pursuant to subsection D of this section, object to production under subsection E of this section or file a motion to quash or modify the subpoena under rule 45 of the Arizona rules of civil procedure.

D. It is sufficient compliance with a subpoena issued in a court or tribunal proceeding if a health care provider delivers the medical records or payment records under seal as follows:

1. The health care provider may deliver by certified mail or in person a copy of all the records described in the subpoena by the production date to the clerk of the court or tribunal or if there is no clerk then to the court or tribunal, together with the affidavit described in paragraph 4 of this subsection.

2. The health care provider shall separately enclose and seal a copy of the records in an inner envelope or wrapper, with the title and number of the action, name of the health care provider and date of the subpoena clearly inscribed on the copy of the records. The health care provider shall enclose the sealed envelope or wrapper in an outer envelope or wrapper that is sealed and directed to the clerk of the court or tribunal or if there is no clerk then to the court or tribunal.

3. The copy of the records shall remain sealed and shall be opened only on order of the court or tribunal conducting the proceeding.

4. The records shall be accompanied by the affidavit of the custodian or other qualified witness, stating in substance each of the following:

(a) That the affiant is the duly authorized custodian of the records and has authority to certify the records.

(b) That the copy is a true complete copy of the records described in the subpoena.

(c) If applicable, that the health care provider is subject to the confidentiality requirements in 42 United States Code sections 290dd-3 and 290ee-3 and applicable regulations and that those confidentiality requirements may apply to the requested records. The affidavit shall request that the court make a determination, if required under applicable federal law and regulations, as to the confidentiality of the records submitted.

(d) If applicable, that the health care provider has none of the records described or only part of the records described in the subpoena.

5. The copy of the records is admissible in evidence as provided under rule 902(11), Arizona rules of

evidence. The affidavit is admissible as evidence of the matters stated in the affidavit and the matters stated are presumed true. If more than one person has knowledge of the facts, more than one affidavit may be made. The presumption established by this paragraph is a presumption affecting the burden of producing evidence.

E. If a subpoena does not meet one of the requirements of subsection B of this section or if grounds for objection exist under rule 45 of the Arizona rules of civil procedure, a health care provider may file with the court or tribunal an objection to the inspection or copying of any or all of the records as follows:

1. On filing an objection, the health care provider shall send a copy of the objection to the patient at the patient's last known address, to the patient's attorney if known and to the party seeking the records, unless after reasonable inquiry the health care provider cannot determine the last known address of the patient.

2. On filing the objection, the health care provider has no further obligation to assert a state or federal privilege pertaining to the records or to appear or respond to a motion to compel production of records, and may produce the records if ordered by a court or tribunal. If an objection is filed, the patient or the patient's attorney is responsible for asserting or waiving any state or federal privilege that pertains to the records.

3. If an objection is filed, the party seeking production may request an order compelling production of the records. If the court or tribunal issues an order compelling production, a copy of the order shall be provided to the health care provider. On receipt of the order, the health care provider shall produce the records.

4. If applicable, an objection shall state that the health care provider is subject to the confidentiality requirements in 42 United States Code sections 290dd-3 and 290ee-3, shall state that the records may be subject to those confidentiality requirements and shall request that the court make a determination, if required under applicable federal law and regulations, on whether the submitted records are subject to discovery.

F. IF A SUBPOENA MEETS ONE OF THE REQUIREMENTS OF SUBSECTION B OF THIS SECTION, A HEALTH CARE PROVIDER MAY FILE THE MEDICAL RECORDS OR PAYMENT RECORDS UNDER SEAL PURSUANT TO SUBSECTION D OF THIS SECTION OR SHALL PRODUCE THE MEDICAL RECORDS OR PAYMENT RECORDS TO THE PARTY SEEKING THE RECORDS. IF PRODUCED TO THE PARTY SEEKING THE RECORDS, THE RECORDS SHALL BE ACCOMPANIED BY THE AFFIDAVIT OF THE CUSTODIAN OR OTHER QUALIFIED WITNESS, STATING IN SUBSTANCE THE ELEMENTS SET FORTH IN SUBSECTION D(4) OF THIS SECTION.

G. IF RECORDS PRODUCED UNDER SUBSECTION D OR SUBSECTION F OF THIS SECTION ARE ACCOMPANIED BY THE AFFIDAVIT PRESCRIBED BY SUBSECTION D(4) OF THIS SECTION, THE HEALTH CARE PROVIDER NEED NOT COMPLY WITH A NOTICE OF DEPOSITION OF THE CUSTODIAN OF RECORDS, UNLESS SO ORDERED BY A COURT OR TRIBUNAL.

~~F.~~H. If a party seeking medical records or payment records wishes to examine the original records maintained by a health care provider, the health care provider may permit the party to examine the original records if the subpoena meets one of the requirements of subsection B of this section. The party seeking the records also may petition a court or tribunal for an order directing the health care provider to allow the party to examine the original records or to file the original records under seal with the court or tribunal under subsection D of this section.

I. THIS SECTION APPLIES TO ANY PERSON OR ENTITY THAT MAINTAINS OR HANDLES MEDICAL RECORDS OR PAYMENT RECORDS, OR INFORMATION CONTAINED IN MEDICAL RECORDS OR PAYMENT RECORDS, ON BEHALF OF A HEALTH CARE PROVIDER.

6) Adult Day Health Care Facility Regulations (ADHS)

A.A.C. R9-10-511(C)

Description of Laws:

A.A.C. R9-10-511(C) requires adult day health care facilities to have medical records "recorded in ink."

Identified Barriers to Health Information Exchange:

A record "recorded in ink" presumably does not permit adult day health care facilities to use electronic health records. While the intent was undoubtedly to prohibit these facilities from keeping medical records with pencil or other non-permanent medium, the language used seems to require hand-written records.

Proposed Solution:

This regulation should be updated to permit electronic health records.

R9-10-511. Participant Records

A. The administrator shall ensure that up-to-date participant records are available to the participant or participant's representative upon 48 hours' written notice to the facility, excluding weekends and holidays.
B. Records for each participant shall include the following:
1. Full name, date of birth, social security number, and address;
2. Names, addresses, telephone numbers of participant's representative, medical provider, and other medical and nonmedical providers involved in the care of the participant;
3. Enrollment agreement;
4. Emergency information;
5. Written acknowledgment of the receipt of copies of participant rights and facility rules;
6. Signed medical provider's assessment;
7. Medical provider's orders;
8. Evidence of freedom from tuberculosis;
9. Comprehensive assessment;
10. Records of medical care and medications provided by the facility;
11. Vital signs and nutritional status;
12. Care plan;
13. Documentation of any significant changes in participant behavior or condition, including injuries and accidents, and notification of the participant's medical provider and participant's representative;
14. Signed authorization if medical information is released;
15. Determination of participant's capability of signing in or out of the facility; and
16. Discharge date, if applicable.

C. Records shall be legibly recorded ~~in ink~~. Each entry shall be dated and signed. Records shall be protected at all times from possible loss, damage, or unauthorized use.
D. Records shall be retained for three years.
E. If the facility ceases operation, copies of records shall be available upon the request of the participant or participant's representative for three years from the date of closure.

(7) Arizona Health Care Cost Containment System (AHCCCS) Regulations:

A.R.S. § 36-2901 and A.A.C. R9-22-512

Description of Laws:

Statutory and regulatory restrictions apply to disclosures by the Arizona Health Care Cost Containment System (AHCCCS) and organizations that are AHCCCS contractors, providers, and noncontracting providers.[27] The AHCCCS plan and its contractors, providers and noncontracting providers may disclose information related to AHCCCS applicants, eligible persons or members in more limited circumstances than permitted by the HIPAA Privacy Rule.[28] Significantly, the regulations require the holder of a medical record of a "former applicant, eligible person, or member" to obtain written consent from that person "before transmitting the medical record to a primary care provider."[29] On the other hand, "subcontractors are not required to obtain written consent from an eligible person or member before transmitting the eligible person's or member's medical record to a physician who: (1) provides a service to the eligible person or member under subcontract with the program contractor, (2) is retained by the subcontractor to provider services that are infrequently used or are of an unusual

[27] A.R.S. § 36-2901 (definitions).

[28] A.A.C. R9-22-512 permits disclosures of information concerning an "eligible person, applicant, or member" only:

(1) To the individual;
(2) With authorization of the individual (where the authorization meets certain requirements);
(3) To persons or agencies for "official purposes" related to administration of the AHCCCS program. These "official purposes" include establishing eligibility and post-eligibility treatment of income; determining the amount of medical assistance; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the AHCCCS program; performing evaluations and analyses of AHCCCS operations; filing liens on property as applicable; filing claims on estates; filing, negotiating, and settling medical liens and claims; and providing services for eligible persons and members. "[P]roviding services for eligible persons and members" is read broadly to permit disclosure for "treatment, payment and health care operations," as defined under HIPAA, and to family members or friends involved in the treatment of the member;
(4) For "official purposes" related to administration of the AHCCCS program and only to the extent required in performance of duties, to employees of AHCCCS, the Social Security Administration, Arizona DES, ADHS, the federal DHHS, the Arizona Attorney General's Office, the Board of Supervisors, AHCCCS eligibility offices, and the County Attorney, as well as employees of contractors, program contractors, providers and subcontractors.
(5) To law enforcement for the purpose of an investigation, prosecution, or criminal or civil proceeding relating to the administration of the AHCCCS program, including where the member is suspected of AHCCCS fraud or abuse (and otherwise if the law enforcement official has statutory authority to obtain the information);
(6) To a review committee pursuant to A.R.S. § 36-2917; and
(7) To the extent required in the performance of duties to various government agencies.

[29] A.A.C. R9-22-512(G).

nature, and (3) provides a service under the contract."[30] The regulations also do not expressly permit release of AHCCCS member information for research purposes.

Identified Barriers to Health Information Exchange:

Information about AHCCCS members will be included in HIE; indeed, AHCCCS itself is creating an HIE for AHCCCS providers. The current regulations pose the following barriers to including AHCCCS member information in an HIE:

A.A.C. R9-22-512(3) permits disclosures of information concerning an "eligible person, applicant, or member" to persons or agencies for "official purposes" related to administration of the AHCCCS program. The "official purposes" listed include "establishing eligibility and post-eligibility treatment of income; determining the amount of medical assistance; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the AHCCCS program; performing evaluations and analyses of AHCCCS operations; filing liens on property as applicable; filing claims on estates; filing, negotiating, and settling medical liens and claims; and providing services for eligible persons and members." While we believe that the phrase "providing services for eligible persons and members" is read broadly to permit disclosure for "treatment, payment and health care operations," as defined under HIPAA, and to family members or friends involved in the treatment of the member, we urge AHCCCS to consider clarifying that conclusion in its regulatory revisions.

A.A.C. R9-22-512(4) permits release of information "official purposes" related to administration of the AHCCCS program and only to the extent required in performance of duties, to employees of AHCCCS, the Social Security Administration, Arizona DES, ADHS, the federal DHHS, the Arizona Attorney General's Office, the Board of Supervisors, AHCCCS eligibility offices, and the County Attorney, as well as employees of contractors, program contractors, providers and subcontractors. We recommend that AHCCCS consider permitting release of information to ADHS and county public health officials for public health purposes.

A.A.C. R9-22-512 does not expressly permit release of AHCCCS member information for research purposes. We recommend that AHCCCS consider including this in the regulation.

To raise a broader issue, we urge AHCCCS to reconsider whether this regulation should apply to health care providers. Because health care providers are already required to follow a plethora of federal and state statutes and regulations governing the privacy of health information, we strongly AHCCCS to remove providers from the scope of this regulation.

We have not proposed suggested language, as we want to work collaboratively with AHCCCS on appropriate changes to its regulations.

---

[30] A.A.C. R9-22-512(H).

Exhibit E

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework:
HIE Legislation—Enforcement and Safe Harbors

November 13, 2007 Meeting Agenda (1-4 pm)

1. Welcome and introductions

2. Overview of work done on HIE legislative issues to date and status

3. Articulation of concerns related to HIE enforcement and safe harbors
    a. Consumers
    b. Providers
    c. HIE
    d. Payors
    e. Others

4. Development of principles to apply to enforcement/safe harbor framework
   See Connecting for Health, *Architecture for Privacy in a Networked Health Information Environment*

5. Discussion of present enforcement and safe harbor provisions in federal and state law
   See chart

6. Discussion of need for additional legislation
    a. Is legislation on these issues necessary?
    b. If yes, on what issues?
    c. If yes, who are the interested stakeholders that we need to involve?

7. Next steps

8. Other Business

Exhibit F

Arizona Health-e Connection Legal Working Group
Development of a Framework for Enforcement and Safe Harbors

Existing Federal and Arizona Laws Relating to Enforcement of Unauthorized Access to Health Information and Protection for Appropriate Use by Health Care Providers

FEDERAL HEALTH-RELATED LAWS

Citation	Summary
HIPAA	
Privacy Rule, 45 CFR Part 160, Part 164, Subpart E	Detailed requirements regarding appropriate internal use and external disclosure of protected health information
Security Rule, 45 CFR Part 160, Part 164, Subpart C	Detailed requirements regarding the administrative, technical, and physical security procedures required to protect electronic protected health information
42 USC 1176	Civil penalties: not more than $100 for each violation, up to a total of $25,000 for all violations of an identical requirement or prohibition during a calendar year
42 USC 1177	Criminal penalties: "A person who knowingly and in violation of this part--(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person" may: "(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."
Enforcement Rule, 45 CFR Part 160, Subpart C	Procedural rules for enforcement of civil penalties
Substance Abuse Treatment Regulations	
42 CFR Part 2	Detailed requirements regarding the use and disclosure of information by a federally-assisted drug or alcohol abuse treatment program
42 USC 290ee-3(f), 42 USC 290dd-3(f), 42 CFR 2.4 42 CFR 2.5	Criminal penalties: Not more than $500 for a first offense; not more than $5,000 for each subsequent offense

Medicare Conditions of Participation	
42 CFR 482.13 Patient Rights COP	482.13(c)(1) (patient right to personal privacy); 482(d)(1) (patient right to confidentiality of clinical records)
42 CFR 482.24 Medical Records COP	482.24(b) (requiring system of author identification and record maintenance to ensure the integrity of the authentication and protects the security of all record entries); 482.24(b)(3) (requiring procedure for ensuring the confidentiality of patient records)

FEDERAL COMPUTER-RELATED LAWS

Citation	Summary
18 U.S.C. 1028 Identity Theft	Punishes a person who knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document that is or appears to be issued by or under the authority of the United States or the production, transfer, possession, or use is in or that affects interstate or foreign commerce, including the transfer of a document by electronic means Penalties: a fine or imprisonment of up to 30 years (depending on the circumstances), or both

18 U.S.C. 1030 Computer Fraud	Punishes fraud and related activity in connection with computer, for anyone who:
	• intentionally accesses a computer **without authorization** or **exceeds authorized access** and obtains information from any **protected computer** if the conduct involved an interstate or foreign communication (§ 1030(a)(2)(C))
	  • the term **'protected computer'** means a computer which is used in interstate commerce or communication (§ 1030e)(2)(A))
	• knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and furthers the intended fraud and obtains anything of value (§ 1030(a)(4))
	• knowingly causes the transmission of a program, information, code, or command, and as a result, intentionally causes **damage** without authorization, to a protected computer (§ 1030 (a)(5)(A)(i))
	  • the term '**damage**' means any impairment to the integrity or availability of data, a program, a system, or information. (e)(8)
	
	Penalties: a fine or imprisonment of up to 20 years (depending on the circumstances), or both

ARIZONA HEALTH-RELATED LAWS (Applicable to Providers)

Citation	Summary
ARS 12-2291, *et seq.* Medical Records Laws	No enforcement agency or penalties for violation specified. Immunity for good faith compliance: ARS 12-2296 ("A health care provider or contractor that acts in good faith under this article is not liable for damages in any civil action for the disclosure of medical records or payment records or information contained in medical records or payment records that is made pursuant to this article or as otherwise provided by law. The health care provider or contractor is presumed to have acted in good faith. The presumption may be rebutted by clear and convincing evidence."
ARS 12-2801, *et seq.* Genetic Testing Information	No enforcement agency or penalties for violation specified. Immunity for good faith compliance: ARS 12-2802(G) ("A health care provider and the provider's agents and employees that act in good faith and that comply with this article are not subject to civil liability. The good faith of a health care provider that complies with this article is presumed. The presumption may be rebutted by a preponderance of the evidence.")
ARS. 36-135 and A.A.C. R9-6-708 Immunization Information	ARS. 36-135 "F. A health care professional who provides information in good faith pursuant to this section is not subject to civil or criminal liability. G. A health care professional who does not comply with the requirements of this section violates a law or task applicable to the practice of medicine and an act of unprofessional conduct. H. Any agency or person receiving confidential information from the system who subsequently discloses that information to any other person is guilty of a class 3 misdemeanor."
ARS 36-501, *et seq.* Mental Health Information	No enforcement agency or penalties for violation specified; no immunity specified
ARS 36-661 *et seq.*, Communicable disease information	ARS 36-666. Violation; classification; immunity A. A person who knowingly does the following is guilty of a class 3 misdemeanor: 1. Performs, or permits or procures the performance of, an HIV-related test in violation of this article. 2. Discloses, compels another person to disclose or procures the disclosure of communicable disease related information in violation of this article. B. A person, health facility or health care provider disclosing communicable disease related information pursuant to or required by this article is immune from civil or criminal liability if the person, health care facility or health care provider acted in good faith and without malice. C. A health facility or health care provider, including a physician, the physician's employer or the health care facility or health care provider with which the physician is associated, is immune from civil or criminal liability for failing to disclose communicable disease related information to a contact or a person authorized pursuant to law to consent to health care for a protected person if the health facility or health care provider acted in good

	faith and without malice. D. For the purposes of this section, good faith and the absence of malice are presumed unless the presumption is overcome by a demonstration of clear and convincing evidence to the contrary. 36-667. Civil penalty A. The department may impose a civil penalty of not more than five thousand dollars if a person does the following in violation of this article: 1. Performs, or permits or procures the performance of, an HIV-related test in violation of this article. 2. Discloses, compels another person to disclose or procures the disclosure of communicable disease related information in violation of this article. B. The director shall deposit, pursuant to sections 35-146 and 35-147, all monies collected pursuant to this section in the state general fund. 36-668. Private right of action A protected person may bring an action in superior court for legal and equitable relief on his own behalf against a person who violates this article.
Various	State licensure regulations for various health care organization and licensed health care professionals require confidentiality, and are enforceable through licensure proceedings

ARIZONA COMPUTER-RELATED LAWS

Citation	Summary
A.R.S. 13-2008 Identify Theft	A person commits taking the identity of another person…if the person knowingly takes, purchases…records, possesses, or uses any personal identifying information of another person, without the consent of that other person…with the intent to obtain or use the other person's identity for any unlawful purpose or to cause loss to a person whether or not the person actually suffers any economic loss as a result of the offense (13-2008 (A)) Violation of the section is a class 4 felony (13-2008 (E))
A.R.S. 13-2009 Aggravated Identity Theft	A person commits aggravated identity theft when it involves identity theft of five or more individuals or entities (13-2009) Violation of the section is a class 3 felony (Id.)
A.R.S. 13-2010 Trafficking	A person commits trafficking in the identity of another person…if the person knowingly sells, transfers or transmits any personal identifying information…without the consent of the other person…for any unlawful purpose or to cause the loss to the person…whether or not the other person or entity actually suffers any economic loss (13-2010(A)) Violation of this section is a class 2 felony (13-2010(C))
ARS 13-2316 Computer Tampering	A person who acts without authority or who exceeds authorization of use commits tampering by…Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by…a medical institution. (13-2316 (A)(7) Violation of this section is a class 6 felony (13-2316 (E))

ARS 13-2316.01 Access Device	A person commits unlawful possession of an access device by knowingly possessing …or controlling an access device without the consent of the owner or authorized user and with the intent to use or distribute that access device (§13-2316.01 (A)) "Access device" means any…account number…personal identification number, password, encryption key, biometric identifier or other means of account access that can be used…to obtain…access. (13-2301(E)(2)) Unlawful possession of one hundred or more access devices is a class 4 felony. Unlawful possession of five or more but fewer than one hundred access devices is a class 5 felony. Unlawful possession of fewer than five access devices is a class 6 felony. (13-2316(C))
ARS 13-2316.02 Unauthorized release of confidential computer security information	A person commits unauthorized release of proprietary or confidential computer security information by communicating, releasing or publishing proprietary or confidential computer security information…relating to a particular computer, computer system or network without the authorization of its owner or operator (13-2316.02 (A)) Violation of this section is a class 6 felony (13-2316.02(D))
ARS 44-7501 Security Breach Reporting	Requires an owner or licensor of **unencrypted computerized data** that includes **personal information** that becomes aware of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, to conduct a reasonable investigation to promptly determine if there has been a breach of the security system. A breach in the security system, requires notice to the individuals affected (in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system). Notice is required by: 1. Written notice. 2. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229; 114 Stat. 464; 15 United States Code section 7001). 3. Telephonic notice. 4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following: (a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice. (b) Conspicuous posting of the notice on the web site of the person if the person maintains one (c) Notification to major statewide media. Enforcement: The attorney general may bring an action to obtain actual damages for a willful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

	Exceptions: 1. A person subject to the Gramm-Leach-Bliley Act; and 2. HIPAA covered entities Definitions: 1. "Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further willful unauthorized disclosure. 3. "Encrypted" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. 4. "Individual" means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach. 5. "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include the department of public safety, a county sheriff's department, a municipal police department, a prosecution agency or a court. 6. "Personal information": (a) Means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (i) The individual's social security number. (ii) The individual's number on a driver license issued pursuant to section 28-3166 or number on a nonoperating identification license issued pursuant to section 28-3165. (iii) The individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. (b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. 8. "Redact" means alter or truncate data such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information.

Exhibit G

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework:
HIE Model Participation Agreement and Policies

Summary of November 13, 2007 Meeting

Attendees: Beth Schermer, Kristen Rosati, Eric Thomas, Patricia Henrikson, Laura Carpenter, Anita Murkco, Mike Stearns, Jackie Heitzman, Marissa Castro, Lynn Golder, Perry Yastrov, Bill Pike, Mary Kay McDaniels, Matt Devlin, Jeremy Stoloff, Kim Snyder and Emilie Sundie

1. **Welcome and Introductions**
   Beth Schermer and Kristen Rosati of Coppersmith Gordon Schermer & Brockelman PLC chaired the meeting. The meeting participants introduced themselves.

2. **Best Practices Subgroup Report**
   Ms. Schermer reviewed the Best Practices Subgroup on Model Policies and Participation Agreements summary report and key findings. The survey included health information exchange initiatives in Long Beach, California; Tennessee (CareSpark); Utah (Utah Health Information Network); Delaware; Washington state (Inland Northwest); Vermont; Indiana (Regenstrief Institute); and Massachusetts (MA-Share). With few exceptions (Indiana and Massachusetts), most of the exchanges contacted were still in start-up mode, focusing on limited exchange of clinical information. The specific scope of health information available through the exchange and the range of participating providers varied significantly between exchanges based upon readily available resources.

   With respect to patient consent practices, the survey did not reveal a strong trend on opt-in, opt-out or no- consent from patients for the transfer of their data for treatment purposes. The group discussed the Indiana and Massachusetts's experiences with consent issues at length.

3. **Model Participation Agreement**

   AHCCCS and Southern Arizona Health Information Exchange (SAHIE) provided an update on the status of their HIE development work. AHCCCS intends to implement Phase I of its work, a health information exchange, in June of 2008. The planned exchange will allow for participating providers to initially access hospital discharge summaries, medication history, lab results from Sonora Quest and LabCorp, and advance directives from the Secretary of State. AHCCCS is planning a controlled launch with a limited set of AHCCCS provider participants. Phase II of the AHCCCS project will include provider access to a patient electronic medical record.

   SAHIE reported that it has narrowed its review of HIE development proposals to three vendors. SAHIE is looking at the ability of these vendors to support administrative transactions, a clinical data exchange, and e-prescribing services. SAHIE anticipates that a vendor will be selected in January, and that meetings regarding implementation can begin immediately after that. It hopes to initiate limited information exchange in the summer of 2008. Both AHCCCS and SAHIE hope to link their exchanges through a single portal.

The group reviewed key issues for the draft Provider Participation Agreement:

- The purpose of the agreement as drafted is to allow the exchange of patient information for medical treatment and health care services to patients. The group discussed at length whether the authorized purpose should be expanded to include research, and reached a consensus that the initial agreement will focus on medical treatment and health care services only. The agreement will be drafted to include addenda for expanded use at a later time. While research-based information use would be beneficial to providers, the exchange and consumers, the group felt that consumer trust in the exchange process would be stronger if the initial work was limited to medical care and treatment. In addition, the group concluded that the agreement should reflect no competitive "business uses" of the information in the HIE (which would be difficult, given that HIEs will limit access to only one patient record at a time).

- The group discussed whether and how to seek patient consent to transfer information through an HIE. The group noted that federal and Arizona law did not require patient consent for the exchange of health information between providers for treatment purposes. Moreover, even HIEs that have stricter state laws on patient consent (such as Massachusetts), permitted the exchange of health information through an HIE for treatment purposes. While the group felt that transparency to consumers of information exchange for treatment purposes is important, the group also felt that it would be more beneficial for treatment purposes not to seek express patient consent, as many individuals would not have the opportunity to consent until health care was needed (such as in the ED), and because more limited information would make the HIE less useful to providers and thus reduce its use. Moreover, there are substantial costs and administrative issues involved in administering the consent process. However, the group agreed to continue to study the consent issue in light of its sensitivity and the importance of consumer acceptance.

- The agreement will be divided into sections that apply to healthcare provider participants who access the data in the HIE, and other data participants that provide data to the HIE, such as SureScripts.

- The agreement will be revised to allow for exchange between HIEs for treatment purposes.

- The group agreed that the agreement should include additional details from the draft policies.

- The group concluded that participants should have the responsibility to document what information was secured from the HIE and relied upon for medical decision making, and that there should be flexibility in how this is done (for example, by printing out hardcopy of information, downloading information or entering notes describing information reviewed). This is required to comply with the Arizona law regarding what constitutes a "medical record," which includes records generated by third parties that are relied upon by a provider to provide treatment.

- The agreement provisions on confidentiality of other date (proprietary information) will be maintained but shortened.

- The termination provisions will reflect that data stored before provider participant termination will not be removed from the HIE, and will continue to be available for treatment purposes.

- The group discussed indemnification issues and concluded that indemnification based upon common law would be the guiding principle (i.e. that all parties would be responsible for their own acts or omissions).

4. Model Policies

Patient Consent: AHCCCS has established an internal working group to address this issue. The AHCCCS group has not reached a decision, but Mr. Devlin noted that if the use of information is limited to patient care, the "no-consent" option has strong advantages. After considerable discussion, the LWG agreed to draft the policies based on a "no-consent" placeholder, but recognized that the issue would require further study and stakeholder input.

Other Policies: Because of limited time, Ms. Schermer asked that LWG participants provide comments on the other draft policies by telephone, email or mail before the next LWG meeting.

5. Process for Stakeholder Review of Agreement and Policy Drafts

Ms. Schermer outlined the next steps of document revision and stakeholder input:

- The agreement and draft policies will be revised and circulated to LWG for further review and comment, along with a draft notice for consumers on information use.

- LWG, through AzHEC, would work with the Arizona Hospital and Healthcare Association to distribute the draft documents to hospitals' counsel for feedback.

- LWG, through AzHEC, would work with ArMA and other medical associations and societies to distribute the draft documents to physicians and their representatives for feedback.

- LWG, through AzHEC, would work with the AzHEC Consumer Advisory Council to secure feedback on the documents

Exhibit H

MEMORANDUM

DATE: October 9, 2007

TO: Best Practices Subgroup (Kim Harris-Salamone, Pat Henrikson, Carolyn Rose, Perry Yastrov, Rob Lindley, Bill Pike)

FROM: Beth Schermer and Kristen Rosati

RE: HIE Best Practices Survey/Model Policies and Participation Agreement

Thank you for serving on the Best Practices Subgroup. The Subgroup has been asked to contact operational health information exchanges (HIEs) across the country to gather information on best practices for model policies and participation agreements.

Background

The Legal Working Group is developing a "common framework" for HIE activity in Arizona. The common framework is based upon the following assumptions:

1. The HIE will initially provide a record locator function for participating providers.

2. The HIE will allow access to limited health information, such as discharge summaries and laboratory test reports.

3. Participating providers will include physicians, hospitals and laboratories. Payors will not be included in this first phase.

4. Participating providers can be both data providers and data users.

5. Data use will be limited to patient care and treatment.

Our immediate goal is to develop by December 2007:

1. Provider Participation Agreement. We will develop a standardized form of HIE provider participation agreement. This initial document will run between the HIE and participating providers.

2. Core Policies. We will develop a standardized set of core policies for HIE provider participation. These policies will address:

    - Patient consent/consumer rights
    - Participating provider registration and authentication
    - HIE access and data use
    - HIE data submission
    - HIE auditing and compliance

AzHEC intends that the Provider Participation Agreement and Core Policies will be used for the AHCCCS Phase I HIE initiative and the SAHIE effort as it develops.

Best Practices Survey

The Legal Working Group asked that a Best Practices Subgroup be formed to survey operational HIEs around the country to gather information on core policies and sample provider participation agreements. The issues of patient consent and consumer rights are critical to the success of the HIE effort. As a result, the survey is to focus on these specific issues, while at the same time collecting basic information on other policy issues and agreement terms.

We have prepared a survey tool for this process, which is attached to this memorandum. We have also identified HIEs for contact and have assigned specific HIEs to subgroup members. The HIE contact sheet and suggested assignments is included with this email. If you have any concerns with your contacts or would like to change assignments, please let us know.

We would appreciate your contacting the HIEs and providing us with your responses by Monday October 22. We will be scheduling a telephone conference to discuss results later that week.

Best Practices Subgroup
Questions on Policies, Consent,
Model Agreements and Enforcement

October 8, 2007

1. Brief Summary of Organization Functions

   - What health information is provided to the HIE?
   - Where stored?
   - Who provides the information?
   - Who has access?
   - For what purpose?
   - How is the information exchanged?
   - What is the current status of the HIE
     - Such as number of active participants, records
     - Additional phases/future plans
   - Does the HIE have written policies
     - If yes, on what topics?
     - Will you share the policies?

2. Patient Consent Policy

   - How do you handle patient consent—general provisions?
     - Opt in, opt out, no consent, other arrangement?
     - If consent, what does it cover:
       - Putting information into HIE, use of information through HIE, disclosure to third parties?
     - At what stage or stages do you secure patient consent?
   - Details on how is consent secured
     - Who secures consent?

- How is consent secured—electronically or otherwise?
- For what – by treatment episode or for all future treatment?
- Can patient direct a limit on what goes in or goes out?
- How is consent managed – through IT? Who maintains?
  - ♦ Where is consent documented and kept?
  - ♦ What uses and intervals are covered under the consent?
  - ♦ Who updates or amends consent, and how?
  - ♦ How does provider verify consent?
  - ♦ How does a patient revoke consent?
- What are state law requirements for consent?
  - ♦ If not required, why does HIE secure consent?

▪ Process

- Any documents describing process?
- What type of stakeholder input did you secure to make policy decisions? How?

3. Other Policies

▪ What other policies does the HIE have

▪ Share?

4. Model Participation Agreement

▪ Does HIE have a participation agreement for data providers?

▪ Does HIE have a participation agreement for data users?

▪ Share sample agreement(s)?

5. Enforcement?

▪ Private action

- If data provider or data user violates policy/agreement – what is response?

    - Third party (insurer, other individual, provider, employer) improper access – what response?

- State action
    - Any state laws providing enforcement? Civil or criminal?
    - Describe law and penalties
    - Has HIE used enforcement provisions yet?
    - Who do they target? (Any third party access? Insurer, employer, provider, hackers?)
    - Who is left out?
    - Funding for enforcement?

Exhibit I

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**[1]
Type of health info provided to the HIE	"DOCS4DOCS® service is an independent, community-based clinical messaging service. It electronically delivers test results and other clinical information securely and efficiently. It is used in 28 hospitals in Indiana, which send approximately one million messages each month to 5,000 physicians." (See http://www.ihie.com/docs4docs.html) IHIE also operates "The Quality Health FirstSM program, a clinical quality program for health and chronic disease management, built on the DOCS4DOCS® service functionality. The community	The Regenstrief Institute operates this repository, where "mirrors" of participants' EHRs held in separate "silos".	Conducting HIE pilot in three communities, in which EHRs have been provided to all community physicians. Northern Berkshire is the first operating HIE, as all physicians adopted the same EHR platform. All information in this chart is about the Northern Berkshire HIE. Medications, allergies, current medical problems, recent test results, some history, and other summary information is presented in an "eHealth Summary." (The information in the physician's EHR is only available to that office.)

[1] MA-SHARE, a subsidiary of the Massachusetts Health Data Consortium (MHDC), also is working on HIE issues. MA-SHARE conducted the " MedsInfo ED pilot" and is now conducting an e-prescribing pilot. MHDC is a member of the Massachsetts e-Health Collaborative.

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**[1]
	service provides standardized quality measures used by physicians and health insurers to help monitor chronic diseases and common preventative health screenings. By combining medical and drug claims data from participating health plans with patient prescription drug data, lab and test results from the Indiana Network for Patient Care database and the DOCS4DOCS® service, the Quality Health FirstSM program creates reports that physicians can use to better monitor and improve the health of their patients."		
Where info is stored	Stored in central repository by IHIE.	Stored in central repository.	eHealth Summary is stored in central repository.
Who provides the info	Hospitals	Participating hospitals and physicians	Physicians and acute care hospital in North Adams, Mass.
Who has access to the info	Participating hospitals and physicians	Participating hospitals and physicians	Physicians and nurses (and office staff with limited access to

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**[1]
			demographic information)
Purposes for which the info may be accessed	Treatment	Treatment. The Regenstrief Institute also utilizes the information in the repository for research purposes (after appropriate IRB approval).	All legally permitted uses and disclosures (clinical care, billing and financial management, administrative management, reports to public health agencies and other governmental requirements, reports to protect the security of medical information, reports to evaluate the use of eHealth Summary, and reports to track and evaluate the quality of health care services)
How the info is exchanged	Unknown	Upon query about a particular patient by a participant, the system pulls relevant information from the participants' EHRs to create a clinical abstract for that patient. The participant can also pull particular records referenced in the clinical abstract, directly from the participants' EHR.	Via eHealth Summary
Current status of HIE (e.g. number of active participants)	Currently operational—28 hospitals and 5,000 physicians.	Currently operational	Northern Berkshire is a small community of 45,000 people. Northern Berkshire Healthcare (NBH) including North Adams Regional Hospital (NARH) a 120 bed community hospital and the

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**[1]
			only acute care facility in the area; Visiting Nurses Association and Hospice of Northern Berkshire; Sweet Brook Transitional Care and Living Centers; Sweetwood Continuing Care Retirement Community and REACH Community Health Foundation. The hospital has 80 active medical staff including 32 primary care physicians and 48 specialists.
Topics of written HIE policies	Unknown		Consent Policy: http://www.maehc.org/documents/LevelsofConsent-Final_000.pdf Consent Form: http://www.maehc.org/documents/ConsentFormlores_000.pdf Monitoring and sanctions policy: http://www.maehc.org/documents/PrivacyandSecurityMonitoringandSanctionsv5_000.pdf Mitigation and notification policy: http://www.maehc.org/documents/MitigationandNotificationPolicyforPrivacyandSecurityViolationsv21_000.pdf Confidentiality agreement for employees to sign: http://www.maehc.org/documents/ConfidentialityAgreement-Final_000.pdf Security login form: http://www.maehc.org/documents/SecurityLoginAccountForm-FINAL.pdf Community communication brochure:

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative[1]**
			http://www.maehc.org/documents/EHealthRecordlores_000.pdf
Other			--

PATIENT CONSENT POLICY Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**
How patient consent is handled (opt in, opt out, no consent)	No patient consent is obtained	No patient consent is obtained. (INPC used to have an opt-out policy, but this was phased out when no patients opted-out of the program.)	For the eHealth Summary in Northern Berkshire HIE, opt-in consent is sought. No consent is sought for exchange of orders and results delivery.
If consent is required, what does it cover (putting info into HIE, using info from HIE, disclosing info to 3rd parties)	NA	NA	Consent to include health information in the eHealth Summary, and to use information for the purposes outlined above.
Stage when patient consent is secured	NA	NA	Consent obtained once by patient's physician on behalf of all providers.
Details on how consent is secured (electronically or otherwise?)	NA	NA	In writing.
What the consent covers (treatment episode or all future treatment)	NA	NA	All future information.
Patient's ability to limit info in HIE	NA	NA	None

Survey of Other Health Information Exchanges (HIEs)

PATIENT CONSENT POLICY Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**
Who manages and maintains consent (IT?)	NA	NA	Unknown.
Where consent is documented and kept	NA	NA	Unknown.
Uses and intervals covered under the consent	NA	NA	All treatment.
Who updates and amends consent	NA	NA	Unknown
How a provider verifies consent	NA	NA	Unknown
How a patient revokes consent	NA	NA	Unknown
State law requirements for consent (if none, why does HIE secure consent)	Indiana law does not require patient consent for use and disclosure of patient health information for treatment purposes.	Same	Massachsetts law requires consent for disclosure of certain sensitive information, some of which may be included in the eHealth Summary.
Stakeholder input for policy decisions – type and method	Unknown	Unknown	Unknown.

OTHER POLICIES/MODEL PARTICIPATION AGREEMENT Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**
Other HIE policies	--	--	See above
Participation agmt for data providers	Yes	Yes	Yes
Participation agmt for data users	Yes	Yes	Unknown

Survey of Other Health Information Exchanges (HIEs)

ENFORCEMENT Exchanges 1-3			
	Indiana Health Information Exchange	**Indiana Network for Patient Care**	**Massachusetts eHealth Collaborative**
Private action; State action (civil or criminal? Penalties)	Unknown	Unknown	Unknown
Who enforcement targets (3rd party access, insurers, employers, providers)	Unknown	Unknown	Auditing and enforcement policy
Whether HIE has used any enforcement provisions	Unknown	Unknown	Unknown
How enforcement is funded	Unknown	Unknown	Unknown

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
Type of Health info provided to the HIE	Patient summary data (highly available data and highly desirable data) – meds, allergies, labs, ICD9 codes, CPT codes, and discharge summaries.	Not yet operating.	Administrative Data.	Provides access to general educational info.	Health summary, meds, allergy list. Utilize a common patient identifier.	Lab info, medications, demographics, and chronic disease mngmt. 2 EDs (3 EDs and 5 health centers within a year).
Where info is stored	Everyone who is big enough to store its own data (hospitals) will have its own encrypted tunnel on the data center with the HIE server.	Central repository has de-identified data; hybrid, hospitals maintain their own data (competitive issues).	Web services hub.		No record locator system. Instead have a master patient index that links the info which can be in a doctor's office, lab, or hospital.	Hybrid. Centralized and also in application. History is federated.
Who provides the info		Hospitals, docs, labs (no images yet), public health, eventually - payers			Hospitals provide docs access to data. For some docs, now provide HL-7 messaging to their EMRs. Most info is	PBMs provide medication history. Primary care docs provide info.

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
					outbound and they're now working on bi-directional data sharing.	
Who has access to the info	Pilot project restricted to providing data to EDs; anyone doing triage and treatment in the ED can access the data (cannot be accessed from outside of the ED). Are determining whether to print the data in which case it will be available to clerks who will put the data in the patient's chart so the physician need not look it up.	Docs, hospitals, and eventually patients.	Encryption separate from authentication. UHIN authenticates the bricks –and-mortar physical location; names one person a site administrator and gives that person a login and password – that person makes the password confidential from UHIN; the site administrator authorizes users who each have their own login and password which is		38 hospitals, 400 registered docs (but 1000 docs can get data), 25 clinics. No health plans are included. Provide ad hoc reports to public health re surveillance and public health trends.	Some participants.

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
			confidential from the site administrator.			
Purposes for which the info may be accessed	Patient care in EDs (biosurveillance and emergency preparedness are keys, public health is body in charge which helps alleviate community concerns)	Care delivery. Looking at using the central repository for research.		Treatment of patients; collection of payment for services provided to patients; conducting business operations; complying with health care laws. May not use the info for benefit of 3rd parties.		
How the info is exchanged	Using ADT data to pre-populate (go back 6 months to a year) and 6 months of lab data. Will first set up Edge Servers so data is collected immediately while the RLS is fine-	Electronically via a document registry (RLS). There is also a clinical document repository (clinical encounters) and data repository (discrete data elements).			Electronically.	Internet based exchange.

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
	tuned. Will use MedPlus, the First Gateway Solution for 3 years.	Primarily through provider IS/EMR. Will be providing a portal for docs without EMRs.				
Current status of HIE (e.g. number of active participants)	Don't have any signed agmts; not yet functioning; just have first funding.	Not yet operating.	Has been running for some time (incorp. In 1993).		Started as shared services organization 14 yrs ago; moved to shared IT services 9 years ago for 38 hospitals; then evolved into data sharing. Believe that strong business case and participant needs must be drivers of HIE. 2.6 million records are in the hospital foundation. Working on bi-directional info transfer.	Approx 5,000 records are exchanged per month (should go to 35,000 in a year). Plan to expand provider participation.

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
Topics of written HIE policies		Info control, data sharing. They are basing the policies on MA-SHARE, Indianapolis, Columbus, and CalRHIO – will share with us when they're complete.			Policies are defined in contract participant signs to become part of the program. They will check into whether they can share the policies with us.	Privacy, company sanctions, employee manual. Will share with us and have shared with Indianapolis. They'd like the report we generate from these interviews.
Other			Vendors: HTP Incorporated, Direct Pointe		Vendors: Epic, Meditech (hospital system), Centricity. Closest model to them is Health Bridge in Cincinnati and Utah model which started with the support of payers to share administrative data.	

Survey of Other Health Information Exchanges (HIEs)

BRIEF SUMMARY OF ORGANIZATION FUNCTIONS Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
					Santa Barbara tried to do too much all at once.	

Survey of Other Health Information Exchanges (HIEs)

PATIENT CONSENT POLICY Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
How patient consent is handled (opt in, opt out, no consent)	Data use agmt covers consent for treatment purposes; no consent for now because it's limited to EDs, will use opt out when it expands outside of EDs	Consent and privacy is participant's responsibility. The HIE monitors, provides abuse info, and maintains the consent info.	Data provider is responsible for obtaining "all required patient authorizations for the transmission of patient info."		Opt-out on a form. Primary care docs give permission to specialists to access patient info.	Opt-in. Patients are told about the program and its advantages. They can then check a box and sign the form.
If consent is required, what does it cover (putting info into HIE, using info from HIE, disclosing info to 3rd parties)		Providers' discretion.				
Stage when patient consent is secured		At point of care.			Each provider secures patient consent at entry into health care delivery system.	At each provider site.
Details on how consent is secured (electronically or		Providers obtain a signed agmt and then enter it electronically.	Each provider is responsible for its own privacy.			On paper with an electronic indication that the patient

Survey of Other Health Information Exchanges (HIEs)

PATIENT CONSENT POLICY Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
otherwise?)						signed the form. Heavy emphasis on patient education of the advantages of participation – signs in lobbies, waiting rooms, brochures.
What the consent covers (treatment episode or all future treatment)		One time consent for all content.				Current and future treatments.
Patient's ability to limit info in HIE		By provider, all or nothing for each provider.			No exceptions.	None.
Who manages and maintains consent (IT?)					Still evolving.	
Where consent is documented and kept					Still evolving.	At each provider site. Vermont law requires each site to have a consent form on record.
Uses and		Provider			Still evolving.	

Survey of Other Health Information Exchanges (HIEs)

PATIENT CONSENT POLICY Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
intervals covered under the consent		discretion.				
Who updates and amends consent					Still evolving.	
How a provider verifies consent					Still evolving.	
How a patient revokes consent					Still evolving.	The patient has to work it out with each provider.
State law requirements for consent (if none, why does HIE secure consent)		There are a few problematic laws being amended. Consent is required for certain types of info and there are limitations on sharing.	Utah security/privacy laws outside of HIPAA are minimal.			
Stakeholder input for policy decisions – type and method		Focus groups.			Evolved out of the shared services program. INHS is part of the North/West RHIO which helps	Providers, MD advisory group, consumers, health plans, State government.

Survey of Other Health Information Exchanges (HIEs)

PATIENT CONSENT POLICY Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
					prioritize INHS processes.	

OTHER POLICIES/MODEL PARTICIPATION AGREEMENT Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
Other HIE policies	Their security policies are HIPAA security policies from one of their partners.	Personnel policies, business associate agmts, and background checks – will share when complete.				Will share.
Participation agmt for data providers	None.	Data sharing agmts.				Yes. Will share.
Participation agmt for data users	None.	Phased approach: 1. Public health. 2. Exchange of clinical data for treatment purposes. 3. De-identified				Yes – member agmt and payer agmt. Will share.

Survey of Other Health Information Exchanges (HIEs)

OTHER POLICIES/MODEL PARTICIPATION AGREEMENT Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
		for 2ndary use (not to be used for revenue). CareSpark will not do research. Whoever is doing research will need to recruit providers and patients to have their data involved.				

ENFORCEMENT Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
Private action; State action (civil or criminal? Penalties)	The HIE will have a physician and patient privacy board that will review and respond to any breaches. This board will have	No state laws specifically addressing e-health.		If monitoring reveals possible evidence of criminal activity, evidence may be provided to law enforcement for criminal	The participation agreement defines each participant's responsibilities and violations of the contract are handled as	Don't have authority to take action. Each site follows own policy re privacy protection. Consumers can call an 800

Survey of Other Health Information Exchanges (HIEs)

ENFORCEMENT Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
	authority to notify the medical boards or hospitals of any breaches.			prosecution and may be used for administrative action. Info on the system is subject to the Privacy Act of 1974, 5 USC 552a and misuse may be subject to a fine of up to $5k plus CP.	private actions. No state laws re protecting personal information. State laws are a little more restrictive than HIPAA.	number which is forwarded to the provider or site where the problem occurred. State Ombudsman program registers complaints.
Who enforcement targets (3rd party access, insurers, employers, providers)	Auditing every week, looking for a single person with unusually high volume, requiring docs to declare a relationship with the patient, initially will physically compare lists of ED patients with HIE activity	If unintentional and not malicious, then reprimand. Provider/hospital must deal with problem. If it continues, may shut-off access and alert the State. Will still take the data but will not allow access to HIE.				
Whether HIE has used any		No.			No.	No problems have surfaced.

Survey of Other Health Information Exchanges (HIEs)

ENFORCEMENT Exchanges 4-9						
	Long Beach Network for Health	**CareSpark**	**Utah Health Information Network**	**Delaware Health Information Network**	**Inland Northwest Health Services (INHS)**	**Vermont Information Technology Leaders**
enforcement provisions						
How enforcement is funded						

Exhibit J

Coppersmith Gordon Schermer & Brockelman PLC

MEMORANDUM

DATE: August 17, 2007

TO: Arizona Health-e Connection Legal Working Group

FROM: Beth J. Schermer and Kristen B. Rosati

RE: Arizona Health Privacy Project Phase II – Development of Model Provider Participation Agreement and Policies for HIE

The Legal Working Group of the Arizona Health Privacy Project will hold a series of meetings this fall to develop a Model Provider Participation Agreement and Model Policies and Procedures to support the development of health information exchanges in Arizona. The development of these model documents represent the second phase of activity under the Health Information Security and Privacy Collaboration grant, and will support the development of health information exchanges in Arizona.

This memorandum describes the proposed process to develop these documents, the timetable for these activities and an initial summary of key topics the Model Agreement and Model Policies and Procedures.

The first meeting to discuss the Model Agreement and Model Policies and Procedures is **September 18, 2007, 9 a.m. to 12 p.m.** at 1700 West Washington Street, the Tower's First Floor Conference Room. Please RSVP to Kim Snyder before September 16 at ksnyder@azgita.gov or voice mail at 602-364-4795

We hope that you will be able to attend and participate in this important initiative! If you know others that would like to be involved in this effort, please feel free to forward this memorandum.

Background

The Arizona Health Privacy Project was launched in June 2006 with the Health Information Security and Privacy Collaboration (HISPC) contract to identify security and privacy practices in Arizona that would affect the establishment of health information exchanges (HIEs) or regional health information organizations (RHIOs) in the state. The Project identified specific practices and concerns described in its March, 2007 final report, "Privacy and Security Solutions for Interoperable Health Information Exchange: Final Assessment of Variation and Analysis of Solutions." The Project also

presented these findings at the Arizona Health-e Connection Summit on March 20, 2007, which many of you attended.

HIE and RHIO initiatives have continued to gain momentum in Arizona since the filing of the Final Report. The Arizona Health Care Cost Containment System (AHCCCS) was awarded a Medicaid Transformation Grant from CMS for the development of a Medicaid HIE, and is in the early stages of a three-year plan to develop this information exchange. The Southern Arizona Health Information Exchange (SAHIE) has also launched its development efforts and is soliciting vendors to support the HIE and hopes to be operational next year. Other regional health information exchanges are gaining momentum throughout the State.

New Project for the Legal Working Group: Model Agreement and Policies

The Arizona Health Privacy Project is now ready to enter the second phase of work needed to support the development of HIE and RHIO initiatives in Arizona. This work will include the development of key template documents, including a Model Provider Participation Agreement and Model Policies and Procedures. These documents will establish model terms and conditions for provider access to health information and a master provider index. Supported by the Arizona Health-e Connection, the Legal Working Group will spearhead the development of these documents with input from a broad array of stakeholders.

To leverage work done across the country on HIE access agreements, the Legal Work Group will assemble existing resources for the participation agreements, including the Markle Foundation and eHI Connecting Communities materials, to determine the best method for developing a Model Provider Participation Agreement. The goal is to establish a model agreement with broad-based support that will be adopted by Arizona HIEs and RHIOs. We also hope that the Model Provider Participation Agreement and Model Policies and Procedures will support efforts of HIEs and RHIOs across the country.

The Legal Work Group will also continue to work on proposals for statutory and regulatory amendments to state statutes and regulations that pose potential barriers to HIE in Arizona, as identified in Phase One of the Arizona Health Privacy Project, so that access to HIE or RHIOs through the Master Provider Index will be possible. These statutory and regulatory amendment proposals will address communicable disease, mental health, immunization, and genetic testing information, and processes for subpoenas for medical records, as defined in the March 2007 Report. Further, the Legal Work Group will continue to work on creating a new statute governing enforcement/penalties for inappropriate access to a health information exchange (HIE) and immunity for providers and other authorized individuals who access information in a HIE in an appropriate fashion. The status and timetable for that work is explained in a separate memorandum.

Timetable for Development of Model Participation Agreement and Policies

The proposed timetable calls for three meetings of the Legal Working Group to develop a model participation agreement and policies. Coppersmith Gordon will facilitate the Legal Working Group meetings, gather information from a variety of sources for review by the Legal Working Group, draft the key documents and integrate comments, revisions and input from the Legal Working Group as well as other stakeholders.

Date	Activity
Week of 9/10/07	Coppersmith Gordon to circulate list of proposed topics for model policies and participation agreement, and sample model policies and model participation agreements from other sources
9/18/07 9 am -12 pm	Meeting 1: Tentative Agenda: • Review potential HIE structures in Arizona and underlying assumptions • Review and provide feedback on topics for model policies • Review and provide feedback on topics to cover in model participation agreement
Week of 10/8/07	Coppersmith Gordon to circulate proposed detailed outline of model policies and model participation agreement
10/15/07 1pm -4 pm	Meeting 2: Tentative Agenda: • Review and provide feedback on outline for model policies and procedures and recommended terms • Review and provide feedback on outline for model agreement and identified recommended terms
Week of 11/5/07	Coppersmith Gordon to circulate draft model policies and draft participation agreement
11/13/07 9 am-12 pm	Meeting 3: Tentative Agenda • Review and provide feedback on draft model policies • Review and provide feedback on draft model participation agreement

The timetable for this work is ambitious. We will circulate draft documents the week before each meeting and anticipate substantial work between meetings.

Materials for the September 18, 2007 Meeting

We will circulate materials for the September 18, 2007 meeting the week of September 10. In the meantime, if you are interested in reviewing existing resources developed by the Markle Foundation Connecting for Health project and the eHealth Initiative Connecting Communities project, see http://www.markle.org/markle_programs/healthcare/projects/connecting_for_health.php and http://toolkit.ehealthinitiative.org/policies_for_information_sharing/default.mspx (free registration required). Both are excellent resources that we will utilize in this project.

We look forward to seeing you on September 18, 2007. If you have questions or would like to discuss any part of this process, please give contact Beth Schermer or Kristen Rosati.

Beth Schermer
602-381-5462
bschermer@cgsblaw.com

Kristen Rosati
602-381-5464
krosati@cgsblaw.com

Exhibit K

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework: HIE Model Participation Agreement and Policies

September 18, 2007 Meeting Agenda

1. Welcome and introductions

2. Update on Arizona Health-e Connection (AzHEC) and HIE Development in Arizona
    a. AzHEC update
    b. AHCCCS Transformation Grant and HIE Project report
    c. SAHIE report
    d. Overview of Legal Working Group development of the Arizona Common Framework: Model Participation Agreement and Policies

3. Review and discuss potential HIE structures and assumptions

4. Model participation agreement
    a. Identify topics for agreement
    b. Process for identifying other states' agreements and approaches
    c. Timeframe for drafting and review
    d. Process for stakeholder outreach

5. Model privacy policies
    a. Identify topics for model policies
        i. Patient consent for submission of health information to HIE
        ii. HIE participant registration/ authentication and access
        iii. Authorized use of health information in the HIE by participants
        iv. HIE auditing and compliance policy
        v. Other core policies?

    b. Process for identifying other states' policies and approaches
    c. Timeframe for drafting and review
    d. Process for stakeholder outreach
    e. Begin discussion of how/when to seek patient consent

6. Other business

Exhibit L

Arizona Health-e Connection Legal Working Group

Development of the Arizona Common Framework: HIE Model Participation Agreement and Policies
Draft for Discussion September 18, 2007 Legal Working Group Meeting

Summary of Terms and Conditions for a Provider-HIE Participation Agreement*

1. Introduction. A description of the Health Information Exchange or "HIE" and how it is organized and operated, in order to provide information that may be helpful for putting the remainder of the Terms and Conditions into context.

    1.1 Nature of Organization. The legal structure within which the HIE is organized, and the HIE's essential relationships to sponsors, founders and others.

    1.2 Purposes. The purposes for which the HIE is organized.

    1.3 Description of Services. The facilities and services of the HIE that are subject to the HIE Terms and Conditions, and that are available to Participants.

    1.4 Change or Termination of Services. The HIE's right to change its services or to cease providing services. [Note: This might be located in a termination section instead.]

    1.5 Parties. The parties to the Agreement ("Participant" and HIE).

2. Definitions. The definitions of certain important terms used in the Terms and Conditions. Some of these definitions may not correspond to their use in certain other contexts, and are likely to vary if the HIE's organization, operations, system, services and/or relationships with others are different than those assumed by the Model.

    "Authorized User" means an individual Participant or an individual designated to use the HIE's Services on behalf of the Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant's medical staff.

    "Data" means the scope of data covered by HIE Services.

    "Data Provider" means a Participant that is registered to provide information to the HIE for use through the HIE's Services.

*This list of suggested terms and conditions for a model Provider-HIE Participation Agreement is adapted in part from "Key Topics in a Model Contract for Health Information Exchange" prepared by the Connecting for Health Policy Committee in April 2006 as part of The Connecting for Health Common Framework. The Connecting for Health Common Framework is created by the Markle Foundation and funded by Markle and the Robert Wood Johnson Foundation.

This list also reflects topics that have been central in the development of electronic health record use agreements between different types of providers.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder at 45 CFR Parts 160 and 164.

"Participant" means a party that registered with the HIE to act as a Data Provider and/or as a Data Recipient.

"Participant Type" means the category of Participants to which a particular Participant is assigned based upon that Participant's role in the health care system.

"Patient Data" means [individually identifiable patient] information provided by a Data Provider pursuant to the section on Provision of Data.

"Participation Agreement" means a legally-binding agreement between the HIE and a Participant pursuant to which the HIE registers the Participant in accordance with, and the Participant agrees to comply with, the HIE Terms and Conditions.

"HIE's Services" means the information sharing and aggregation services and software described in Section ____ (Description of Services) for which the Participant registers.

"HIE Terms and Conditions" means the terms and conditions set forth in this document, as amended, repealed and/or replaced from time to time as described herein.

"Data Recipient" means a Participant that uses the HIE's Services to obtain health information [or Patient Data].

3. Participant Registration. Who may be a Participant, and how the HIE will register each Participant. The Model uses the concept of "registering" Participants as the device by which the HIE will monitor and control who uses the HIE's System and Services.

[Note: The Legal Working Group should consider whether the registration arrangement will be separate from the Participation Agreement; this outline assumes that registration terms and conditions are incorporated into the Participation Agreement, which is the binding document between the HIE and the Participant as well as Authorized Users identified by the Participant.]

3.1 Registration Required. The requirement that Participants be registered with the HIE.

3.2 Registration Process. How Participants will register (online, by written agreement)

3.3.1 Registration Form. How the Participant accesses the Registration Form.

3.3.2 Participant Type. How the HIE will categorize Participants by their respective roles in the health care system, i.e., for the purpose of determining the rights and obligations of those Participants.

3.3.3 Review and Acceptance of Registration Forms. The HIE's rights to review registration forms and decide whether or not to accept any given party's registration.

3.4 Effect of Participation Agreement Terms and Conditions. How Participants will agree to comply with the Terms and Conditions of the Agreement.

3.5 Changes to Terms and Conditions. How Participants will be made aware of changes made to the Agreement Terms and Conditions, and will be legally obligated to comply with them.

3.6 Termination Based on Objection to Change. How a Participant may terminate participation and registration if the Participant objects to a change to the Agreement Terms and Conditions.

4. Term and Termination. The term of the Agreement and any renewal terms, as well as how the parties can terminate the Agreement and their rights and obligations following termination.

4.1 Participant's Rights to Terminate Agreement. How and under what circumstances a Participant may cease to be a Participant, generally.

4.2 Participant's Right to Terminate for Breach of Business Associate Section of Agreement.. A Participant's rights to terminate an Agreement if the HIE fails to perform any obligations it may have as a business associate (as defined in HIPAA) of the Participant.

4.3 HIE's Right to Terminate Registration Agreements. How and under what circumstances the HIE may terminate a Participant's Agreement.

4.4 Effect of Termination. The consequences of terminating the Agreement.

4.5 Survival of Provisions. The provisions of the Agreement that shall continue to bind the Participant and HIE following termination.

5. Authorized Users. Terms that govern use of the HIE Services by the Participant's Authorized Users. Participants will be responsible for designating the individuals within their organizations who would be authorized to use the HIE's System and Services ("Authorized User").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will use the HIE's Services.

5.2 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users.

5.3 No Use by Other than Authorized Users. A requirement that the HIE's System and Services be accessed and used only by Authorized Users.

5.4 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users.

6. Data Recipient's Right to Use Services. Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the HIE's Services). Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data to the HIE) appear at Section 7 (Data Provider's Obligations).

6.1 Grant of Rights. The nature of the Participant's right to use the System and Services.

6.1.1. Grant by HIE. The rights granted by the HIE.

6.1.2. NHIN. The rights granted by the NHIN, if any.

6.2 Permitted Uses. The permitted uses of the HIE's System and Services.

6.3 Prohibited Uses. The prohibited uses of the HIE System and the HIE Services applicable under the Arizona Common Framework Policies and Procedures, and additional prohibitions imposed by the HIE, if any.

7. Data Provider's Obligations. Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data). Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the HIE's Services) appear at Section 6 (Data Recipient's Right to Use Services).

7.1 Grant of Rights. The nature of the Data Provider's right to use the System.

7.2 Provision of Data. Terms that apply to the Data Provider's delivery of data to the Network, e.g., format, standards, etc.

7.3 Measures to Assure Accuracy of Data. The Data Provider's obligations to provide accurate, complete, and timely information.

7.4 License. The Data Provider's agreement that the data it provides will be available for use through the Network.

7.5 Limitations on Use of Patient Data. Limitations the HIE will impose upon the uses of information provided by Data Providers, including uses prohibited by the Arizona Common Framework Policies and Procedures, state or local laws and regulations specific to the HIE, and other prohibitions the HIE determines are appropriate (but not in conflict with the Arizona Common Framework Policies and Procedures).

8. Software and/or Hardware Provided by HIE. The Model assumes that the HIE will provide certain software and/or hardware Participants would use to access the System ("Associated Software and/or Hardware"). If the HIE does not provide software and/or hardware to Participants, this section would be omitted.

8.1 Description. A description of any software and/or hardware that the HIE will provide to Participants.

8.2 Grant of License. A description of the Participant's right to use the Associated Software and/or Hardware.

8.3 Copying. Restrictions upon the Participant's right to copy software provided by the HIE.

8.4 Third-Party Software, Hardware and/or Services. How the HIE and Participants will address requirements imposed by third-party software, hardware, and/or service vendors.

9. Protected Health Information. Provisions addressing compliance with applicable laws addressing the confidentiality, security and use of patient health information.

9.1 Compliance with Policies and Procedures. Provisions requiring compliance with the Arizona Common Framework Policies and Procedures.

9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security and use laws imposed at the state and/or local level and/or other requirements that the HIE otherwise determines are appropriate (but not inconsistent with the Arizona Common Framework Policies and Procedures).

9.3 Business Associate Agreement. Provisions addressing the HIE's potential role as a business associate of the Participant.

10. Other Obligations of Participants. Additional terms governing the conduct of Participants.

10.1 Compliance with Laws and Regulations. The Participant's obligations to comply with applicable laws and regulations, generally.

10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the HIE System and to notify the HIE of breaches in security.

10.3 Software and/or Hardware Provided by Participant. Provision requiring the Participant to obtain and maintain all hardware and software required to use the HIE's System and Services that are not to be provided by the HIE.

10.4 Viruses and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the HIE's System.

10.5 Training. A description of the training, if any, that the HIE will require the Participant to provide to its personnel.

11. HIE Operations and Responsibilities. Provisions describing the role and responsibilities of the HIE.

11.1 Compliance. The HIE's obligations to require that all Participants agree to be bound by the HIE Terms and Conditions.

11.2 Training. The HIE's obligations to provide training for Participants and/or their Authorized Users.

11.3 Telephone and/or E-Mail Support. The HIE's obligations to provide support for the Participant's use of the HIE's System and/or Services.

11.4 Audits and Reports. Audits the HIE is to perform, and reports it is to provide, to Participants.

11.5 Management Committee. Any role Participants would have in governance or decision-making by the HIE.

11.5.1 Composition. The composition of a body in which Participants would be involved.

11.5.2 Meetings and Responsibilities of Management Committee. The responsibilities of such a body and how often it would meet.

11.5.3 Management Committee Bylaws. How this body would be organized and governed.

12. Fees and Charges. Terms regarding amounts, if any, that the Participant will be required to pay to the HIE in order to use the Services.

    12.1 Service Fees. The HIE's fees, if any, for Participants.

    12.2 Changes to Fee Schedule. Provisions allowing the HIE to change its Fee Schedule.

    12.3 Miscellaneous Charges. Provisions addressing the HIE's ability to charge for additional services.

    12.4 Payment. How and when payment is due and payable.

    12.6 Late Charges. Whether the HIE would impose late charges on delinquent Service Fees and Miscellaneous Charges.

    12.6 Suspension of Service. Whether the HIE would be permitted to suspend services until the Participant pays amounts that are due.

    12.7 Taxes. The party responsible for payment of taxes arising out of the use of the HIE's System and/or Services.

    12.8 Other Charges and Expenses. The extent to which Participants and/or the HIE are responsible to pay for other expenses relating to their respective roles.

13. Proprietary Information. Provisions concerning the parties' respective obligations to preserve the confidentiality of others' proprietary information (i.e., other than health information).

14. Disclaimers, Exclusions of Warranties, Limitations of Liability and Indemnifications. Standard terms directed to avoiding inappropriate legal claims between the parties.

    14.1 Carrier lines. The parties' respective responsibilities with respect to the use of carrier, e.g., telephone lines.

    14.2 No Warranties. The extent to which the HIE disclaims warranties it might otherwise be assumed to be making to Participants.

    14.3 Other Participants. The extent to which the HIE is responsible for uses of information and/or the Network by others.

    14.4 Participant's Actions. The extent to which the Participant assumes responsibility for its own actions or those of its Authorized Users.

    14.5 Unauthorized Access; Lost or Corrupt Data. The extent to which the parties are responsible for others' access to information through the Network, or for misconduct related to the use and/or disclosure of that data, or for the accuracy or completeness of that data.

    14.6 Inaccurate Data. The extent to which the parties are responsible for inaccurate data obtained through the Network.

    14.7 Patient Care. The parties' responsibilities with respect to patient outcomes affected by use of the Network.

14.8 Limitation of Liability. The extent to which the parties' potential legal liabilities to each other are limited.

15. Insurance and Indemnification.

15.1 Insurance. Whether and to what extent the parties are to be required to carry insurance.

15.2 Indemnification. Whether and to what extent the parties would agree to indemnify each other for losses sustained as a result of their relationships or conduct.

15.3 General Provisions. General provisions appropriate to a contract including the foregoing terms.

Exhibit M

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework:
HIE Model Participation Agreement and Policies

Summary of September 18, 2007 Meeting

1. **Welcome and introductions**
   Beth Schermer and Kristen Rosati of Coppersmith Gordon Schermer & Brockelman PLC chaired the meeting. All participants in the meeting introduced themselves.

2. **Update on Arizona Health-e Connection (AzHEC) and HIE Development in Arizona**
   - AzHEC update – presented by Brad Tritle, Executive Director Arizona Health-e Connection
   - AHCCCS Transformation Grant and HIE Project report – presented by Perry Yastrov, AHCCCS
   - Southern Arizona Health Information Exchange (SAHIE) report – presented by Bill Pike, Carondelet Health
   - Overview of Legal Working Group development of the Arizona Common Framework: Model Participation Agreement and Policies – presented by Beth Schermer and Kristen Rosati

   NOTE: If you would like copies of these presentations please email ksnyder@azgita.gov

3. **Assumptions for the Model Policies and Model Participation Agreement**
   The group was asked to discuss the assumptions for an HIE that would be the basis for developing the model participation agreement and the model privacy policies.
   - Who has access: Scope of initial work will be limited to access to an HIE by providers. Issues related to access for health plans, public health and research are necessary to resolve, but group agreed we would focus on providers first.
     - We need to address physician and office staff access. Hospital experience shows that physicians may provide allow staff to use physicians' access codes if the staff is not provided separate access codes.
   - Who provides information: We will assume that providers, plans and patients may submit information to the HIE.
     - We will assume that the submitter of the information will be responsible for ensuring the completeness and accuracy of the submitted information.
   - What information is provided: We will focus on a subset of clinical data that is likely to be presented through a "patient health summary" or "continuity of care record." This will include patient demographics, present medications, allergies, major health conditions, hospital discharge summaries, next of kin, and health plan coverage. While we eventually will need to address the complete exchange of electronic health records, "interoperability" of EHR is still in the future and may pose more substantial legal issues.
   - We will need to address patient consent for inclusion of information in the HIE, what type of consent will be sought, who will collect, and how that will be administered.

4. Topics to Include in Model Policies

The group then discussed what topics we could cover in the model policies. The following topics were offered, which will be "grouped" in policy categories after the meeting by Coppersmith Gordon.

- HIE Participant Registration/Authentication
  - Who authenticates a user?
  - How is a user authenticated?
  - What will the registration process be?
- HIE Data Provision
  - Who provides the data?
  - What will the terms be for providing the data, including data accuracy requirements?
- HIE Access
  - Who manages access?
  - Who has access? Is it based on a person's role?
  - What internal training requirements will be required?
  - What internal discipline/enforcement requirements will be required?
  - What internal computer security requirements will be required?
- Permitted Uses of HIE Information
  - For what purpose will the information be accessed?
- Consumer Rights
  - How will we address patient consent to include information in an HIE? Opt in/ Opt out/ No Consent? (In Arizona, the federal and state laws do not require consent, other than for disclosure of genetic testing information and substance abuse treatment information that is held by federally-assisted substance abuse treatment programs.)
  - Will consumers have access in the HIE?
  - Notice regarding who will have access to health information?

Creation of Best Practices Task Force: Kim Harris-Salamone (HSAG), Pat Henrikson (Banner Health), Carolyn Rose (Health Choice CEO), Perry Yastrov and Rob Lindley (AHCCCS), Bill Pike (SAHIE) volunteered to work with Beth Schermer and Kristen Rosati to address policy content. They will interview various operating HIEs to collect policies and information about how the consent issue is handled.

5. Model Participation Agreement

- We will be working from the Markle Foundation, Common Framework model agreement.
- We will create one agreement for data providers and data users.
- We will need to address enforcement issues: termination rights, revocation of access and penalties for inappropriate access.
- We will use the AHCCCS model phase one as the HIE model on which we will base the first draft of the participation agreement. We may need to adjust this plan as the AHCCCS plans evolve and when SAHIE announces the HIE model chosen.

Creation of Participation Agreement Task Force:
Matt Delvin, Bill Pike, Dr. Anita Murcko, Mary Beth Joublac and Laura Carpenter agreed to meet with Beth Schermer and Kristen Rosati to draft the agreement for consideration by the committee.

Exhibit N

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework: HIE Model Participation Agreement and Policies

October 15, 2007 Meeting Agenda

1. Welcome and introductions

2. Best Practices Subgroup update on model policies and provider participation agreements

3. Model Policies—Discussion of policy elements

    a. Patient consent/consumer rights
    b. Participant registration and authorization
    c. Data use
    d. Data submission
    e. Audit and compliance

4. Model Participation Agreement

    a. Review of participation agreement outline
    b. Discussion of specific legal issues (outside scope of model policies)

        (1) Liability issues—Participant and HIE responsibilities
            (a) Unauthorized submission of Data
            (b) Unauthorized use of Data
            (c) Liability arising out of inaccurate or incomplete Data
            (d) Other adverse patient outcomes arising out of use of HIE

        (2) Indemnification and Insurance
            (a) Participants' obligations to secure insurance
            (b) Indemnification obligations

        (3) Other business

Exhibit O

ARIZONA HEALTH-E CONNECTION LEGAL WORKING GROUP
POLICY ELEMENTS
DRAFT 10/10/07

[Note: Policy elements subject to revision based upon Best Practices Survey information.]

Glossary:

- Data means Patient health information provided to the HIE by Data Providers and accessible to Authorized Users.
- Authorized User means a Healthcare Provider and its personnel who are authorized to use the HIE to access Data for the purposes of patient care and treatment.
- Data Provider means a Healthcare Provider who provides Data to the HIE.
- Healthcare Provider means a participating physician, hospital, laboratory, or other provider of treatment and related services..
- HIE means health information exchange.
- Participant means a Authorized User or Data Provider.
- Patient means an individual receiving treatment from a Participant.

I. Patient Consent & Consumer Rights

A. Patient Consent for Submission of Health Information to HIE - Options. **[Option and specific elements will be determined following Best Practices Survey]**

1. Opt-in;
2. Opt-out; or
3. No consent required.

Policy should cover:

- What Participant/entity administers opt-in or opt-out process and secures relevant document (broadly called the "consent document" in this policy)
- Timing and duration of opt-in or opt-out
- Form of consent document
- Maintenance of consent document
- Access to consent document
- Data covered by the consent document
- Restrictions on Data subject to consent document
- Revocation/amendment of consent document

B. Notice of HIE Practices.

1. *Content*.
   a. Description of the HIE.
   b. What Data may be included in the HIE. **[Note: Under a patient health summary/ Web portal function, Data initially will include laboratory results, medications, and hospital discharge summaries. May expand to include allergies and other treatment information.]**
   c. Who can access the Data and for what purposes the Data may be accessed. **[Note: At present, Authorized User will have access to Data for care and treatment of Patient.]**
   d. **[If opt-in or opt-out approach adopted, how the Patient can have his or her Data removed from the HIE. Note: Process will have to be identified for removing Data (or limiting access even if Data not removed.]**
   e. **[If technology permits, whether/how the Patient can have access to the Data submitted to HIE.]**

2. *Provision to Patients*. The Notice will be:
   a. Maintained by the HIE and available to the public through the common portal.
   b. Provided to a Patient by a Participant at the date of first service delivery after Participant's agreement to participate in the HIE.
   c. Provided to a Patient by a Participant upon request.

3. Inclusion of HIE Content in Participant Notice of Privacy Practices.
   a. Participants should consider including an explanation of their participation in the HIE in their HIPAA Notice of Privacy Practices (use the explanation provided by

the HIE). **[Note: This is not required, because the release of information by the Data Providers will be for treatment purposes only, and the HIPAA Notice of Privacy Practices is not required to include a description of the specific providers that receive health information nor the method of disclosing information to those providers.]**

II. HIE Participant Registration & Authentication

[Elements will be determined in cooperation with the Arizona Health Privacy Project Technical/Clinical Work Group. Note: At the outset, we need to determine what rules apply to a "Participant" (a legal entity), and the Participants' "Authorized Users".]

A. Authentication. Authorized Users will be authenticated by providing an identifier and a confidential password. This identifier will identify the specific Participant. **[Note: We need to discuss whether dual-factor authentication (i.e. something a Participant knows plus something the Participant has) will be required.]**

1. *Identifier*.
    a. An identifier is an attribute that points unambiguously and uniquely to the identity of a specific Participant.
    b. It is critical that identifiers are not re-issued to other, later Participants.
    c. [Who issues identifiers?]

2. *Password*.
    a. **[Insert rules for secure password for use by Authorized Users.]**
    b. **[Who issues passwords? Participant? HIE?]**

B. Authorization. After an Authorized User claiming a given identity has been authenticated, an authorization mechanism will determine what Data the Authorized User is allowed to access for the purpose of care and treatment of an Authorized User's Patients. Authorization is role-based, and access will be tied to the Authorized User's role. However, because initial use is limited to Patient care and treatment, and Authorized Users are limited to Healthcare Providers and office personnel at a Participant, role based distinctions will be fairly narrow.

C. Employees/Agents/Contractors. Each Participant will follow uniform minimum authentication requirements for verifying and authenticating Authorized Users within its organization who will have access to, and others who request access to, Data through the HIE.

II. HIE Data Use.

A. Patient Access. When the technology becomes available, there will be a formal process through which a Patient may request his or her own Data from the HIE. In the interim period, Participants will make a Patient's HIE record available to the Patient.

B. Participant Access. **[Note: Again, we need to determine what rules apply to a "Participant" (a legal entity), and the Participants' "Authorized Users".]**

1. *Participant Use of Data*. An Authorized User may access Data only for care and treatment of Participant's Patients.

2. *Employees/Agents/Contractors*. Each Participant will allow access to the HIE only by those workforce members, agents, and contractors (Authorized Users) who have a legitimate and appropriate need to use the HIE to secure Data related to the Participant's care and treatment of the Patient.

3. *Training*. Each Participant must develop and implement a training program for its Authorized Users who will have access to the HIE. The training will include a detailed review of applicable policies. All Authorized Users must sign a certification that he or she received, read, and understands these policies before access to the HIE is granted. **[Note: access granted by whom? HIE? Participant?]**

4. *Discipline for Non-Compliance*. Each Participant must implement procedures to discipline and hold Authorized Users accountable for ensuring that they do not use, disclose, or request health information except as permitted by HIE policies and that they comply with HIE policies. The discipline measures should include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.

5. *Reporting of Non-Compliance*. Each Participant must have a mechanism for, and must encourage, all Authorized Users to report to the Participant any noncompliance with its policies. Each Participant will report any noncompliance to the HIE. **[Note: Do we want to place any limitations on this?]** Each Participant also will establish a process for Patients whose Data is included in the HIE to report any non-compliance with these policies or concerns about improper disclosures of their Data **[to whom?]**.

C. Compliance with Law.

1. Each Authorized User will provide or request Data through the HIE for treatment purposes, **[only to the extent necessary]** as permitted by applicable federal, state, and local laws and regulations and these Policies.

2. Data may not be requested for marketing or marketing-related purposes without specific Patient authorization. **[Note: Do we want to consider a complete**

prohibition here? After all, the HIE will also include information provided by multiple Participants, and many Participants will not be comfortable with any use for marketing, even with authorization.]

3. Under no circumstances may Data be requested for a discriminatory purpose.

4. **[Discuss applicability to current Data elements]** If applicable law requires that certain documentation exist or that other conditions be met before using or disclosing Data for a particular purpose, the Authorized User requesting the Data must demonstrate that it has obtained the required documentation or met the requisite conditions and must provide evidence of that documentation at the request of the HIE.

D. Employees/Agents/Contractors. Each Participant may share Data obtained through the HIE with and allow access to the information only by Authorized Users who need the information in connection with their job function or duties relating to the provision of care and treatment to the Patient.

III. HIE Data Submission.

A. Participants. Participants initially providing data to the HIE:
   1. Physicians.
   2. Hospitals **[discharge summary]**.
   3. Laboratories
   4. Prescription health information exchanges.

B. Accuracy. Participants must provide accurate Data to the HIE. **[Note: Do we want to say instead, "Participants may not provide Data to the HIE that they know is not accurate."]**

C. Amending Information. Each Participant must comply with applicable federal, state and local laws and regulations regarding patient rights to request amendment of Data. **[Note: This will depend on the specific architecture that is developed. For example, the patient health summary accessed through the HIE Web portal may be "transient" and pull from the Data Providers' records upon request. In other words, there may not be an HIE "record" to amend.]**
   - **[Will all amendments to Data take place only through Data Provider?]**
   - **[HIE to require that Data Provided provide notice to HIE of amended Data and make amended Data available to HIE if original Data were provided to HIE and is stored by the HIE?]**
   - **[Should the HIE require each Data Provider to have policy for amendment consistent with laws and regulations or should there be a common HIE policy?]**

D. Limiting Information Provided to HIE. If a Participant agrees to a Patient's request for restrictions, as permitted under the HIPAA Privacy Rule, the Participant must ensure that it complies with the restrictions when Participant provides Data to the HIE. If an agreed-upon restriction will or could affect the Authorized User's uses and/or disclosures of Data, the Data Provider must notify the HIE of the fact that certain Data has been restricted, without disclosing the content of the restricted Data**. [Note: We'll need to confirm that this is possible to communicate this through the HIE. More than likely, we'll need to regulate this at Data provision.]**

E. Special Information. Some Data may be subject to special protection under federal or state laws and regulations (e.g., substance abuse treatment information held by federally-assisted substance abuse treatment programs, psychotherapy notes, and genetic testing information). The HIE will determine and identify special protection that may apply to Data under applicable law and notify Data Providers of these restrictions. Each Data Provider will be responsible for identifying Data subject to these special protections and following HIE rules regarding providing this Data to the HIE.

IV. HIE Auditing & Compliance

A. Audit Logs.

1. The HIE will maintain an audit log documenting which Participants provided Data about a Patient, what Authorized Users accessed Data about a Patient, and when the Data was provided and accessed.

2. Upon request, Patients will be able to know who provided Data and who accessed Data relating to that Patient through the HIE and when the information was provided and accessed.

B. Accounting of Disclosures.

1. The HIE will be used only for treatment purposes, for which an accounting is not required.

2. If an Authorized User accesses Data in the HIE for purposes other than for treatment, the Authorized User must inform the HIE of that access of Data. The HIE will then document the access for an accounting, and will provide that accounting to a Participant upon request, so that the Participant can provide that accounting the Patient.

3. The HIE will document all information necessary for compliance with its obligations as a HIPAA Business Associate. Each Participant is responsible for ensuring its compliance with this requirement and may choose to provide Patients with more information in the accounting than is required. Each Authorized User must provide information required for the HIE to meet its obligations as a HIPAA Business Associate. **[Note: The HIE will not have any direct obligations under the HIPAA Privacy Rule.]**

C. Notification of Breach. The HIE will report any serious breaches and/or security incidents to the Participant whose Data was improperly used. Each Participant will inform the HIE of any serious breach of confidentiality. **[The HIE and Participants are not required to inform each other regarding minor breaches.] [Note: We will need to define "serious breach" and "security incident."]**

D. Mitigating Effects of Non-Compliance. Each Participant must implement a process to mitigate, and must mitigate and take appropriate remedial action, to the extent practicable, any harmful effect that is known to the Participant of a use or disclosure of Data through the HIE in violation of applicable laws and/or regulations and/or these Policies by the Participant or its Personnel. Steps to mitigate could include Participant notification to the Patient of the disclosure of Data about the Patient or Participant request to the Authorized User to return and/or destroy the impermissibly disclosed Data.

Exhibit P

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework:
HIE Model Participation Agreement and Policies

Summary of October 15, 2007 Meeting

1. Welcome and Introductions

Beth Schermer and Kristen Rosati of Coppersmith Gordon Schermer & Brockelman PLC chaired the meeting. The minutes from the September 18, 2007 meeting were distributed and reviewed. All participants in the meeting introduced themselves.

2. Best Practices Subgroup Update on Model Policies and Provider Participation Agreements

- LWG participants Kim Harris-Salamone, Pat Henrikson, Carolyn Rose, Perry Yastrov, Rob Lindley, and Bill Pike volunteered to serve on the "Best Practices Subgroup," which will interview other HIEs across the country regarding patient consent and other policy considerations. The LWG reviewed the memo and survey document provided to the Subgroup.
- The Subgroup will report their findings to the LWG in November.
- Kristen reported that there is a national effort to focus on consent issues, through the Health Information Security and Privacy Collaboration multi-state "collaboratives." It is possible that the national efforts will not generate a consensus position, as states that very different laws and policy considerations. The LWG will therefore continue the Arizona process while monitoring national efforts.

3. Model Policies – Discussion of Policy Elements

- Basic Principle. As a general principle, LWG will develop a model participation agreement reflecting HIE polices that establish basic requirements and criteria, in order to minimize the barriers for participants to engage with the HIE and to increase HIE participation.

- Compliance with Laws and HIE Policies: The participant will be required to comply with laws otherwise applicable to the sharing of patient information, as well as specific HIE policies and the participant's own policies.

- HIE-Participant Relationship. The participant will be the legal entity that contracts with the HIE; the participant will have the responsibility for identifying and registering authorized users from its employees and agents, as discussed further below.

- Notice of HIE Practices: The group confirmed that notice to patients that their information would be included in an HIE is important. Notice could be administered differently in different HIEs. For the AHCCCS HIE, for example, notice will be provided to the member upon enrollment. For other HIEs, such as SAHIE, the participant would probably provide notice to the patient upon initial encounter.

- Patient Consent. LWG discussed patient consent process for data exchange:

- The LWG will make recommendations about whether and what type of consent to collect (opt-in, opt-out or none) after reviewing the findings of the Best Practices Subgroup and wider outreach to stakeholders.
- Revocation of consent: An HIE will need a process for communicating revocation of consent and stopping future exchanges of patient information.
- Patients' ability to limit information in the HIE: HIE participants/authorized users will want as much information as possible. The value of information to providers decreases rapidly if portions of a patient's health information are withheld (such as medications). Conversely, patient concerns about privacy may require a process to allow patients to block exchange of specific information, such as mental health information. On balance, the group believes the HIE policies should encourage exchange of full information to the extent possible, and protect privacy through strict rules on access of patient information.

- Responsibility to Document HIE Activity; Use of Specific Data. The LWG discussed how physicians should document reliance on information obtained from the HIE. For example, should they print the information and file or scan it into their record? Should the information be electronically "downloadable" directly into the providers' record? The LWG also discussed what information the HIE could maintain about what information each authorized user accessed, in order to "recreate" the record viewed by the participant.
  - The LWG concluded that participants will be responsible for maintaining a record of what information they accessed for the purpose of treating a patient purposes, by downloading information to electronic record, printing paper copy for record or otherwise noting use of information in their record. Each provider is legally responsible for maintaining the provider's medical record, and it may be very difficult for the HIE to accurate re-create precisely what information was accessed by a provider at a particular time.
  - The HIE will maintain a log of access to information in the HIE. AHCCCS will not keep the actual information accessed; other HIEs, such as SAHIE, may be designed to store data as well as track exchange activity and access. This process will thus vary from HIE to HIE.

- HIE Availability. The LWG discussed availability of HIE information. The goal will be that the HIE can make data available to providers at all times.

- Participant Registration; Authorized User Registration. The HIE will be responsible for participant registration and authentication. The participant will then responsible for registering, authorizing and training individual users ("authorized users"). The LWG agreed that access to the HIE would be role based.
  - The AHCCCS HIE initially will only give access to health care providers. As a result, the need to articulate detailed levels of role- based access will be very limited at this initial stage.
  - The participant will be responsible for identifying authorized users from its employees and agents who need to use the exchange and view data for the purposes of patient care. The participant will be

responsible for monitoring proper use of the exchange and data within its organization.
    - Some hospital electronic health record systems allow clinical connectivity for community physicians and establish contracts with those groups or physicians that provide for termination of the arrangement if the group's employees access information without necessary authorization. The LWG will consider this model for HIE recommended practices.

- Security or Privacy Breach. The LWG discussed breaches by authorized users, what level of breach the participant should report to the HIE, and whether there should be specified levels of required corrective actions. There should be a consistent reporting standard.

- Limitations on HIE Information Use. Initially the exchange will be for exchange of clinical information for treatment purposes. While the uses may expand in the future, the first round of policies and draft participation agreement will focus on this use. The LWG recognized the need to expand uses in some areas, and that this expansion, such as the use of de-identified and aggregated data for research purposes, may provide a means to fund the clinical use of the HIE.

- Data Accuracy and Amendment. Participants should make their best effort to provide accurate data and appropriately amend information. The LWG discussed patients' abilities to amend their information. If data is amended, the participant will need to notify the HIE. LWG agreed that design issues would need to be taken into account to determine if, when, or how HIE might provide notice of amendment to other participants.

- Draft policies will be distributed to the LWG for the November meeting.

4. Model Participation Agreement

- A draft model provider participation agreement will be circulated to LWG for the November meeting. The initial draft agreement will encompass all participating providers under the proposed AHCCCS HIE.

Exhibit Q

Arizona Health-e Connection Legal Working Group
Development of the Arizona Common Framework: HIE Model Participation Agreement and Policies

November 13, 2007 Meeting Agenda

1. Welcome and introductions

2. Best Practices Subgroup report on model policies and provider participation agreements

3. Model Participation Agreement – review of draft agreement

4. Model Policies— review of draft policies

    a. Patient consent/consumer rights
    b. Participant registration and authorization
    c. Data use
    d. Data submission
    e. Audit and compliance

5. Discussion of Process for Stakeholder Review of Agreement and Policy Drafts

6. Other Business

Exhibit R

-Draft for Discussion at November 13, 2007 Legal Working Group Meeting-

ARIZONA HEALTH-E CONNECTION
POLICY DEFINITIONS

- Authorized User means the individuals authorized by the HIE or a Participant to use the HIE to access Data for the purposes of providing medical treatment and health care services to Participant's Patients.

- Data means patient health information provided to an HIE by Data Providers and accessible to Authorized Users. For the purposes of this Agreement, Data means protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

- Data Provider means a Health Care Provider that provides Data to the HIE.

- Health Care Provider means a physician, hospital, ambulatory surgical center, skilled nursing facility, home health care provider, pharmacy, laboratory or other licensed health care provider, which provides medical treatment or health care services to Patients and has entered into an HIE Participation Agreement.

- HIE means health information exchange.

- Participant means a Health Care Provider who has entered into an HIE Participation Agreement, including the Participant named as a party to this Agreement.

- Participation Agreement means an agreement between a Participant and the HIE.

- Patient means an individual receiving medical treatment or health care services from a Participant.

- Policies means these HIE policies.

ARIZONA HEALTH-E CONNECTION
PATIENT CONSENT & NOTICE POLICY

A. Patient Consent for Submission of Health Information to HIE.
]Note: This part of the policy will be created after the LWG makes recommendation on patient consent.]

Policy should cover:

- Whether and what type of patient consent will be required (opt-in, opt-out or none).
- How the patient consent will be administered (by the Participant or HIE?) and how the relevant document is secured (broadly called the "consent document" in this policy)
- What will be the timing and duration of opt-in or opt-out
- What will be the form of the consent document
- Who will maintain the consent document
- Who will have access to the consent document
- What Data will be covered by the consent document—will there be permitted restrictions on the Data covered by the consent
- Will there be permitted restrictions on the authorized users that may see Data
- How will revocation and amendment of the consent document be handled

B. Notice of HIE Practices. The HIE will create a document ("Notice") containing the following information:

1. Description of the HIE. This will include a description of who owns/operates the HIE and where it is located.
2. Description of the Data included in the HIE. For example, if the HIE is limited to handling laboratory results, medications, and hospital discharge summaries, the notice should explain that this information will be available to authorized users
3. Description of what type of individuals are authorized to access Data in the HIE.
4. Description of the purposes for which Authorized Users may access the Data. For example, if the HIE is limited to use for care and treatment, the notice should explain that limitation.
5. Description of how the patient can have his or her Data removed from the HIE (or how Data will be inaccessible for use, even if it is not removed). **[Note: This is only applicable if the HIE adopts an opt-in or opt-out approach to patient consent. .]**
6. How the Patient may requests Data from a Participant. The HIE will not provide access to Data directly to a Patient. Rather, that access will be administered through Participants.
7. Provision to Patients: The HIE will maintain the Notice and make it available to the public through the common portal.
    a. For HIEs that have a direct relationship with the Patient (such as AHCCCS), the HIE will provide the Patient with the Notice upon Patient enrollment or renewal and anytime requested by Patient.

b. For HIEs that do not have a direct relationship wit the Patient, the HIE will require its Participants to provide the Notice to a Patient at the date of first service delivery (after the Participant's agreement to participate in the HIE) and any time requested by a Patient.

ARIZONA HEALTH-E CONNECTION
REGISTRATION & AUTHENTICATION POLICY

A. HIE Authentication of Participant. The HIE will authenticate a Participant by **[describe process developed]**. The HIE will not grant a Participant and its Authorized Users access to the HIE until the Participant signs the Participation Agreement.

B. Participant Determination of Authorized Users. Each Participant is responsible for determining which of its employees and agents will be Authorized Users. A Participant may designate employees and agents as Authorized Users only if they will use the Data in the HIE for the care and treatment of Participant's Patients. This may include employees and agents that are physicians, nurses, other direct care providers, admissions personnel, and other categories of personnel that the Participant documents are involved in the care and treatment of Patients.

C. Participant Training for Authorized Users. The HIE will provide a training program to Participants on HIE use, which will include a detailed reiew of these Policies. Participants will provide this training to all Authorized Users before the Participants permit the Authorized Users ay access to the HIE. Each Authorized User must sign a certification (Training Certificate) that the Authorized User received, read, and understands the Policies and completed the training.

D. Registration of Authorized Users. After an Authorized User completes training and signs the Training Certificate, the Participant may issue an identifier and confidential password to the Authorized User. The Participant will provide the HIE each Authorized User's name and identifier. The HIE will then register each Authorized User.

1. The identifier must point unambiguously and uniquely to the identity of a specific Authorized User and must follow any other directions issued by the HIE for identifiers.
2. A Participant may not re-issue the same identifier to other Authorized Users, even after termination of the first Authorized User.

E. Authentication of Authorized Users. The HIE will authenticate an Authorized User **[describe process developed].** .

F. Termination.

1. Termination of Participant or Authorized User Access By HIE. The HIE will terminate the Participant's or Authorized User's access to the HIE upon one of the following events:
   a. The Participant's or Authorized User's failure to comply with the terms and conditions of the Participation Agreement or HIE policies.
   b. The Participant ceases to be a Health Care Provider.
   c. The Participant's Participation Agreement ends for any reason.

If the action causing termination is related to the act or omission of an Authorized User rather than the Participant, the HIE, in its sole discretion, may terminate the Authorized User directly or may require that the Participant terminate access by the Authorized User.

2. Termination of Authorized User by Participant. The Participant will terminate an Authorized User's access to the HIE upon the following:
   a. The Authorized User ceases to be an employee or agent of Participant.
   b. The Authorized User fails to comply with the terms and conditions for the Participant Agreement or HIE policies.
   c. The determines that the Authorized User no longer has a need to access the HIE relating to provide medical treatment or health care services to Participant's Patients.
   d. The HIE requests that Authorized User's access be terminated for any reason.

3. Notice to HIE. A Participant will notify the HIE immediately when the Participant terminates an Authorized User's access to the HIE. Upon notice of termination, HIE will remove the Authorized User from HIE registration.

ARIZONA HEALTH-E CONNECTION
DATA USE POLICY

A. Patient Access. A Participant must provide a Patient with the Patient's information from the HIE upon the Patient's request.

B. Permitted Purpose of Access. An Authorized User may access Data on the HIE only for the provision of medical treatment or health care services to Participant's Patients.

C. HIE Records. The HIE will maintain a log of Authorized User accessto the HIE.

D. Participant Records. The Participant will be responsible for maintaining a record of the Data its Authorized Users access from the HIE to provide medical treatment or health care services to a Patient. The Participant will determine in which form to maintain its record of Data access. When Data is incorporated into Participant's records, Participant may use and provide access to that Data as permitted by law and will protect the privacy and security of the Data as required by law.

E. Non-Compliance. Each Participant must implement procedures to discipline and hold Authorized Users accountable for violating these Policies or using, disclosing, or requesting a Patient's Data for any reason other than the Permitted Purpose.

1. Discipline. The discipline measures must include, but not be limited to, verbal and written warnings, demotion, and termination. The discipline measures may provide for retraining where appropriate.

2. Reporting Non-Compliance.

   a. A Participant must require its Authorized Users to report to the Participant any noncompliance with the Participation Agreement, these Policies, or the Participant's policies on Data access, use or disclosure.

   b. A Participant must immediately report to the HIE any noncompliance with the Participation Agreement or the HIE's or Participant's policies for Data access, use or disclosure.

   c. Each Participant must have a process for Patients to report to the Participant and any non-compliance with the Participation Agreement, these Policies, and any concerns about Data access, use or disclosure.

ARIZONA HEALTH-E CONNECTION
DATA SUBMISSION POLICY

A. Data Accuracy. Participants may not provide the HIE with Data that they know or should know is not accurate.

B. Amending Data. Each Participant must comply with applicable federal, state and local laws and regulations regarding patient rights to request amendment of protected health information. The Participant should make the amended Data available to the HIE, but is not required to affirmatively report any amendments to the HIE or other Participants.

C. Limiting Data Provided to HIE. If a Participant agrees to a Patient's request for restrictions on the use or disclosure of the Patient's Data, the Participant must comply with these restrictions when providing Data to the HIE. **[Note: If the HIE will not have a mechanism for restricting the use of Data, then the policy should insert:** The HIE will not itself have a mechanism for restricting access to the Data. **If the HIE will have a mechanism for restricting the use of Data and implementing Participants' agreements to restrict with their patients, the policy should insert:** If Data subject to the Participant's agreement to restrict is already in the HIE, the Participant should notify the HIE of the restriction.]

D. Prohibited Data. Participants may not provide to the HIE, Data that are subject to special protection under federal or state laws and regulations. This includes the following:
   1. Substance abuse treatment information held by federally-assisted substance abuse treatment programs;
   2. Ppsychotherapy notes as defined by the HIPAA Privacy Standards, and
   3. Genetic testing information as defined by Arizona Revised Statutes § 12-2801.

   Each Data Provider will be responsible for identifying Data subject to these sp ecial protections and following HIE rules regarding providing this Data to the HIE.

   [Note: if the HIE has a mechanism for restricting access to this special types of information, the policy can permit the Participant to provide this information to the HIE, but then require the Participant to notify the HIE of the special status at submission.]

ARIZONA HEALTH-E CONNECTION
AUDITING & COMPLIANCE POLICY

A. Audit Logs. The HIE will maintain an audit log documenting as to each piece of Data:
   1. when Data was provided to the HIE;
   2. the Participant that provided the Data;
   3. when an Authorized User accessed the Data; and
   4. the Authorized User who accessed the Data and the sponsoring Participant.

   [Note: We should determine whether the HIE will provide a Patient with that Patient's audit log information upon request.]

B. Notification of Breach. The HIE will report any breaches and/or security incidents to the Participant whose Data was improperly used, accessed or disclosed. Each Participant will inform the HIE of any such incidents.

C. Mitigating Effects of Non-Compliance. Each Participant must implement a process to mitigate, and must take appropriate remedial action to the extent practicable, to mitigate any harmful effect that is known to the Participant of improper access, use or disclosure of Data through the HIE in violation of applicable laws, regulations and these Policies by the Participant, Authorized Users or other persons or entities. Mitigation could include Patient notification and Participant's request to the receiving Authorized User to return or destroy the impermissibly disclosed Data.

Exhibit S

-Draft for Discussion at the November 13, 2007
Arizona Health-e Connection Legal Working Group Meeting-

HEALTH INFORMATION EXCHANGE PARTICIPATION AGREEMENT

PARTICIPANT	**[INSERT NAME OF HIE] ("HIE")**
_____	_____
[Address]_____	[Address]_____
[City/State/Zip]_____	[City/State/Zip]_____
[Email]_____	[Email]_____
[Phone]_____	[Phone]_____
[Fax]_____	[Fax]_____

Background:

1. HIE is a [non-profit organization/governmental organization] that owns and operates an Internet-based authenticated system that provides an electronic information exchange (the "Exchange") allowing participating health care provider to exchange clinical data for the medical care and treatment of patients.

2. Participant is a Health Care Provider that provides medical treatment and health care services to patients. Provider seeks to participate in the Exchange in order to secure and provide health care information for the purpose of patient care and treatment.

3. Participant is a [check all that apply]: __ Data Provider __ Data User

Agreement:

1. Services by HIE. HIE manages and administers the Exchange and the use of Data in the Exchange, subject to the Terms and Conditions set forth in Exhibit A.

2. Health Care Provider Participation. Participant may provide Data to the Exchange and access Data in the Exchange ("Data Exchange"), subject to the Terms and Conditions set forth in Exhibit A.

3. Complete Agreement. This Agreement includes, and incorporates by reference, the Agreement, the Terms and Conditions attached as Exhibit A, the HIE Information Security Requirements at Exhibit B, the HIPAA Business Associate Agreement at Exhibit C, and any Project Addendum attached to this Agreement and signed by the Exchange and Participant.

4. Effective Date. The Effective Date for this Agreement is _____.

Participant:	HIE:
By:_____	By:_____

Its:_____ Its:_____

Date:_____ Date:_____

EXHIBIT A
TERMS AND CONDITIONS OF PARTICIPATION

1.0 DEFINITIONS

Authorized User means the individuals authorized by the HIE or the Participant to use the Exchange to access Data for the purposes of medical treatment and health care services to Participant's Patients.

Data means patient health information provided to a HIE by Data Providers and accessible to Authorized Users. For the purposes of this Agreement, Data means protected health information as defined by Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

Data Exchange means electronically providing or receiving Data through the Exchange.

Data Provider means a Health Care Provider who provides Data to the Exchange.

Health Care Provider means a physician, hospital, ambulatory surgical center, skilled nursing facility, home health care provider, pharmacy, laboratory or other licensed health care provider, that provides medical treatment or health care services to Patients and who has entered into an HIE Participation Agreement.

Patient means an individual receiving medical treatment or health care services from a Participant.

Participant means a Health Care Provider who has entered into an HIE Participation Agreement, including the Participant named as a party to this Agreement.

Project Addendum means an exhibit to this Agreement, adopted by the HIE and Participant, that describes a specific project for use of the Exchange, its permitted purpose, applicable standards and safeguards, and related terms.

2.0 HIE OBLIGATIONS

2.1 Compliance. HIE will operate the Exchange in compliance with applicable laws and regulations, including the protection of the privacy and security of Data.

2.2 Policies and Standards. HIE will establish policies and standards (respectively, "Policies" and "Standards") that will govern HIE's and Participant's activity on Exchange, and these Policies and Standards will be available at xxxx.com. HIE encourages Participants to

provide input in the development of Policies and Standards through HIE Participant working groups and committees. These Policies and Standards govern HIE and Participant use of the Exchange and will include Policies for Patient consent, Participant and Authorized User registration and authentication, Data use, Data submission, auditing and compliance, and Standards for matters such as technical operations, connection to the Exchange, and Data Exchange requirements such as format, content and security. Participant will comply with all Policies and Standards as a condition of this Agreement and participation in the Exchange.

(a) Changes to Policies and Standards. HIE may change or amend the Policies and Standards from time to time at its discretion and will post notice of proposed and final changes at xxxx.com. Any changes will be effective 60 days following adoption by HIE, unless HIE determines that an earlier effective date is required to address a legal requirement, a concern relating to the privacy or security of Data or an emergency situation. Participant will have no ownership or other property rights in the Policies and Standards or other materials or services provided by HIE.

(b) Security Standards. HIE will implement Standards that are reasonable and appropriate to ensure that all Data Exchanges are authorized, and to protect Data from improper access, tampering or unauthorized disclosure. Such security Standards will include administrative procedures, physical security measures, and technical security services that are reasonable necessary to secure the Data. HIE and Participant will comply with the security Standards established by HIE, including the requirements set forth on Exhibit B.

(c) Investigations and Corrections. HIE will adopt Policies for the investigation and resolution of Patient complaints, security incidents or other concerns relating to compliance with HIE Policies and Standards and applicable laws ("Compliance Concerns"). HIE promptly will notify Participant in writing of any Compliance Concern related to Participant's use of the Exchange, and Participant will cooperate with HIE in its investigation of any Compliance Concern. **[Note: We need to define Compliance Concern.]**

2.3 Services Provided by HIE. HIE will maintain and operate the Exchange. HIE may contract with subcontractors to maintain and operate the Exchange and HIE will require that its subcontracts comply with the applicable terms and conditions of this Agreement. HIE will maintain records of Data Exchanges as set forth in its Policies and Standards. **[Note: For discussion:** HIE will provide a system of temporary backup of Data Exchanges as required or permitted by law. If Participant is unable to reconstruct Data Exchange or identify Data used for Patient medical treatment or health care services, HIE will assist, at Participant's request and upon payment of HIE fees for such service, in data recovery from such temporary backup systems, provided they are still maintained by HIE.]

2.4 Exchange Availability. HIE will make all reasonable efforts to make the Exchange available to Participants 24 hours a day, 7 days a week; however, Exchange availability may be temporarily suspended for maintenance or unscheduled interruptions. HIE will use its best

efforts to provide reasonable advance notice of any such suspension or interruptions of Exchange availability and to restore Exchange availability.

2.5 Support Services. During the term of this Agreement, HIE will provide support services to assist Participant in the installation, implementation, and maintenance of the software, and use of the Exchange and may establish a fee schedule for these services which will be posted at xxxx.com. The Exchange help desk will be available between ___ a.m. and __ p.m., Monday through Friday, excluding holidays. All such support services will be subject to the HIE budget for such services.

2.6 HIE Use of Data. HIE is not responsible for and will not inspect the content conveyed in Data Exchanges. HIE will not disclose Data or information relating to Data Exchanges to third parties except (a) as provided by this Agreement or as required by law; or (b) as directed in writing by the originating party or intended recipient. HIE may access Data and information relating to Data Exchanges for the operation of the Exchange, testing, performance verification, and investigation of alleged Compliance Concerns.

3.0 PARTICIPANT OBLIGATIONS

3.1 Participants in Exchange; Participation Terms and Conditions. Only Health Care Providers who enter into Participation Agreements may use the Exchange. This Agreement sets forth the terms and conditions for participation in the Exchange and specific projects set forth in any Project Addendum. Participant will be responsible for: (a) its use of the Exchange, including use by Authorized Users identified and authenticated by Participant under HIE Policies; and (b) violations of this Agreement by Participant or its Authorized Users.

3.2 Data Exchange. Participant may participate in Data Exchange as described in the HIE Policies. By engaging in Data Exchange, Participant agrees that (a) its participation in any Data Exchange will comply with the terms and conditions of this Agreement; (b) the Data provided or transferred by Participant can be related to and identified with source records maintained by Participant; and (c) Participant has secured all Patient authorizations for the Data Exchange as set forth in HIE's Policies and Standards and as required by law.

3.3 Permitted Use. Participant and its Authorized Users will use the software and services provided by HIE only to provide Data to or secure Data from the Exchange for the purpose providing medical treatment and health care services to Participant's Patients ("Permitted Purpose"). Participant and its Authorized Users will comply with all applicable laws and regulations governing the privacy and security of Data sent or received in connection with the Exchange. Data received by Participant under this Agreement may become part of Participant's "Designated Record Set" as defined by the federal law. Participant will decide in its discretion whether to use the Exchange, and to what extent.

3.4 Authorized Users. Participant will identify and authenticate its Authorized Users, subject to HIE's Policies, which Authorized Users may use the Exchange for the Permitted

Purpose on behalf of Participant. Authorized Users will include only those individuals who require access to the Exchange to facilitate Participant's provision of medical treatment and health care services to Participant's Patients. Participant is responsible for Authorized Users complying with the terms and conditions of this Agreement.

3.5 Patient Consent for Data Submission and Data Exchange. Participant will secure Patient consent for the Data Submissions and Data Exchange, if required in HIE's Policies and Standards and as otherwise required by law.

3.6 System Operations.

(a) Systems Necessary to Participate in Exchange. Participant, at its own expense, will provide and maintain the equipment, software, services and testing necessary to effectively and reliably participate in the Exchange and engage in Data Exchanges as set forth in HIE Policies and Standards and applicable laws, except for such software expressly provided by HIE pursuant to Section 8.

(b) Record Retention, Storage and Backup. Participant, at its own expense, will maintain Data backup and retention to maintain adequate source records of Data Exchanges and the use of Data as required by law.

(c) Privacy, Security and Accuracy. Participant will maintain sufficient safeguards and procedures, in compliance with HIE Policies and Standards and applicable laws, to maintain the security, privacy and accuracy of Data. Participant will promptly correct any errors discovered in Data Exchanges that it transmits.

4.0 COMPLIANCE WITH LAWS; CHANGE IN LAWS

Both HIE and Participant, and their agents and employees, will comply with the federal and state laws and regulations applicable to this Agreement, including without limitation laws on the security and privacy of Data, Patient consent for the use and transfer of Data and requirements for Data Exchanges.

5.0 FEES AND PAYMENT

6.1 Fees. Participant will pay a program fee ("Fee") to HIE in the amount of _____ _____ ($_____) per calendar quarter/ per month. If this Agreement is in effect for part of a quarter/month, the Fee will be prorated on a daily basis. HIE may modify the Fee from time to time, but such modification will not become effective until Participant has received at least 60 days advance written notice of such modification. Such notice will specify the effective date of the modified Fee.

6.2 Payment. The Fee shall be payable in advance on or before the fifth day of each quarter/month. After 15 days, such payments shall accrue interest at the lesser of 1% per month or the highest rate allowed by applicable law.

6.0 CONFIDENTIALITY

6.1 Proprietary Information. During the term of this Agreement, each party may be given access to information about the other party or that (a) relates to past, present or future business activities, practices, protocols, products, services, data, content, and technical knowledge and (b) has been identified as confidential ('Confidential Information") by such party. For the purposes of this provision, Confidential Information will not include Data.

(a) Non-disclosure. The parties will (a) hold Confidential Information in strict confidence; (b) not make the Confidential Information available for any purpose other than as specified in the Agreement, or as required by law or subpoena; and (c) take reasonable steps to ensure that the Confidential Information is not disclosed or distributed by employees, agents or consultants (who will have access to the same only on a "need-to-know basis) to third parties in violation of this Agreement.

(b) Exclusions. Confidential Information shall not include information which (a) is, at the time of disclosure, known or then becomes known or available to general public through no act of omission of the receiving party which is in violation of such party's obligations under this Agreement; (b) was in the receiving party's lawful possession before such access from the disclosing party; (c) is disclosed to the receiving party by a third party having the right to make such disclosure; or (d) is independently developed by the receiving party without reference to the disclosure party's Confidential Information.

(c) Equitable Remedies. The parties agree that a breach of this Section will cause the disclosing party substantial and continuing damage, the value of which will be difficult or impossible to ascertain, and other irreparable harm for which the payment of damages alone shall be inadequate. Therefore, in addition to any other remedy that the disclosing party may have under this Agreement, at law or in equity, in the event of such a breach or threatened breach by the receiving part of the terms of this Section, the disclosing party shall be entitled, after notifying the receiving party in writing of the breach or threatened breach, to seek both temporary and permanent injunctive without the need to prove damage or post bond.

6.2 Confidentiality of Data. HIE, its agents and employees, and Participant, and its agents and employees, including any Authorized Users, will maintain the confidentiality of Data as required by state and federal law. HIE's use of Data will be subject to the Business Associate Agreement set forth in Exhibit C.

7.0 SOFTWARE LICENSE

HIE grants to Participant for the term of this Agreement a royalty-free, non-exclusive, nontransferable, non-assignable, non-sub-licensable, and limited right to use the software identified by HIE in its technical operation Standards for the sole purpose of participating in the Exchange under the terms and conditions of this Agreement ("Software"). THE SOFTWARE SHALL NOT BE USED FOR ANY OTHER PURPOSE WHATSOEVER, AND SHALL NOT OTHERWISE BE COPIED OR INCORPORATED INTO ANY OTHER COMPUTER PROGRAM, HARDWARE, FIRMWARE OR PRODUCT. THE SOFTWARE IS LICENSED 'AS IS" AND HIE DISCLAIMS ALL REPRESENATATIONS AND WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATIONS, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR TITLE. Participant acknowledges that the Software has been licensed to HIE by third parties, and that the license granted under this Agreement is subject in every respect to HIE's grant of license from such third parties. As additional software is developed by or for HIE for the Exchange, it shall become subject to this Agreement upon written notice to Participant, and such notice shall constitute an amendment to this Agreement and any the applicable Project Addendum. This Section 7.0 applies only to Software that is installed on hardware owned or leased by Participant and not to any other software that Participant may use in providing medical care or treatment to Patients or for Participant's business operations.

8.0 TRANSACTIONS

8.1 Signatures and Signed Documents. Participant, at HIE's request, will adopt as its signature an electronic identification consisting of symbols or codes that are to be affixed to or contained in a Data Exchange made by the Participant ("Signatures"). Participant agrees that any Signature of such party affixed to or contained in any Data Exchange shall be sufficient to verify that the party originated such Data Exchange and the Data included in that transmission. Any properly transmitted Data Exchange made pursuant to this Agreement shall be considered a "writing" or "in writing" and any such Data Exchange when containing, or to which there is affixed, a Signature ("Signed Documents") shall be deemed for all purposes (a) to have been "signed"; and (b) to constitute an 'original' when printed from electronic files or records established and maintained in the normal course of business.

8.2 Validity of Signed Documents. Participant shall not contest the validity or enforceability of Signed Documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the party to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings will be admissible as between the parties to the same extent and under the same condition as other business records originated and maintained in paper form.

9.0 TERM AND TERMINATION

9.1 Term and Termination. The term of this Agreement will begin on the Effective Date and will continue until terminated as set forth in this Section 9.1. This Agreement will terminate under any of the following circumstances:

(a) Violation of Law or Regulation. If either HIE or Participant determines that its continued participation in this Agreement would cause it to violate any law or regulation applicable to it, would place it at material risk of suffering any sanction, penalty, or liability, or would impair its reputation, then that party may terminate its participation in this Agreement on immediate written notice to the other party.

(b) For Cause. If HIE or Participant determines that the other party or any of its agents or contractors have breached this Agreement, including the Terms and Conditions of Participation, then that party may terminate its participation in this Agreement on 15 days' advance written notice to the other party, provided that such notice identifies such area of non-compliance, and such non-compliance is not cured within such 15 day period.

(c) Without Cause. HIE or Participant may terminate this Agreement without cause upon 30 days' advance written notice of termination to the other party.

9.2 Termination Process and Access to Exchange. Upon the effective date of termination of this Agreement, HIE will cease providing access to the Exchange for the Participant and its Authorized Users, and Participant and its Authorized Users will stop using the Exchange. If Participant terminates HIE's rights to access Data controlled by Participant, such Data will no longer be available through the Exchange.

9.3 Effect of Termination.

(a) Rights and Duties. Any termination will not alter the rights or duties of the parties with respect to Signed Documents transmitted before the effective date of the termination or with respect to fees outstanding and payable under this Agreement. Upon termination of this Agreement, Sections _____ shall survive termination of this Agreement, each in accordance with its terms. All other rights, privileges, and responsibilities of each party with respect to the other party shall terminate.

(b) Return of Confidential Information; Software; Fees. Within 30 days of the effective date of termination, each party will return to the other all Confidential Information belonging to the other or certify the destruction of such Confidential Information if agreed to by the party who originated the Confidential Information. Within 30 days of the effective date of termination, Participant will de-install and return to HIE all software provided by HIE to Participant under this Agreement. If Participant has prepaid any Fees or Expenses as of the effective date of termination, Participant will be entitled to a pro rata refund of such advance payment.

10.0 LIMITED WARRANTIES AND DISCLAIMERS

10.1 Limited Warranty and Disclaimer of Other Warranties. HIE will use its best efforts to correctly transmit Data Exchanges between Participant and other Health Care Providers on a timely basis. HIE MAKES NO REPRESENTATION OR WARRANTY THAT THE DATA DELIVERED TO THE PARTICIPANT WILL BE CORRECT OR COMPLETE. HIE MAKES NO WARRANTY OR REPRESENTATION REGARDING THE ACCURACY OR RELIABILITY OF ANY INFORMATION TECHNOLOGY SYSTEM USED FOR THE EXCHANGE. **HIE DISCLAIMS ALL WARRANTIES REGARDING ANY PRODUCT, SERVICES, OR RESOURCES PROVIDED BY IT, OR DATA EXCHANGES TRANSMITTED, PURSUANT TO THIS AGREEMENT INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

11.O LIMITATION OF LIABILITY; INDEMNIFICATION

11.1 Limitation of Liability. Neither HIE nor Participant will be liable to the other for lost profits or Data, or any special, incidental, exemplary, indirect, consequential or punitive damages (including loss of use or lost profits) arising from any delay, omission or error in a Data Exchange or receipt of Data, or arising out of or in connection with this agreement, whether such liability arises from any claim based upon contract, warranty, tort (including negligence), product liability or otherwise, and whether or not either party has been advised of the possibility of such loss or damage. HIE will have no liability for claims based on Participant's use of the Exchange that does not comply with the terms of this Agreement and HIE's Policies and Standards or for claims based upon the content of Data Exchanges.

11.2 Release of Liability. Participant releases HIE and the other Participants from any claim that Participant might otherwise have against any of them arising out of any inaccuracy or incompleteness of the PHI or any delay in the delivery of PHI or failure to deliver a transaction when requested.

11.3 Indemnification.

(a) HIE. HIE will indemnify and hold harmless Participant, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, arising out of claims by third parties that the use of the Exchange and any Software provided by HIE infringes any patents, copyrights or trademarks or is a misappropriation of trade secrets, provided that Participant notifies HIE in writing promptly upon discovery of any such claim and gives HIE complete authority and control of, and full cooperation with, the defense and settlement of such claim.

(b) Participant. Participant will indemnify and hold harmless HIE, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, from claims by third parties arising from claims arising from Participant's unauthorized or

improper use of the Exchange or Participant's or its Authorized Users' use or disclosure of Data for any purpose other than the Permitted Purpose.

11.4 Not a Medical Service. The Exchange does not make clinical, medical or other decisions and is not a substitute for professional medical judgment applied by Participant or its Authorized Users. Participant and its Authorized Users are solely responsible for confirming the accuracy of all Data and making all medical and diagnostic decisions.

12.0 GENERAL PROVISIONS

12.1 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

12.2 Entire Agreement. This Agreement constitutes the complete agreement of the parties relating to the matters specified in this Agreement and supersedes all earlier representations or agreements, whether oral or written with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement is binding on either party.

12.3 No Assignment. Neither HIE nor Participant may assign its rights or obligations under this Agreement without the advance written consent of the other party, except for a transfer or assignment to a parent, subsidiary or affiliate wholly owned by the party.

12.4 Governing Laws. This Agreement is governed by and interpreted in accordance with Arizona laws, without regard to its conflict of law provisions.

12.5 Force Majeure. No party is liable for any failure to perform its obligations in connection with any Data Exchange or activity under this Agreement, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure) which prevents such party from engaging in a Data Exchange or providing or receiving Data.

12.6 Notices. All notices, requests, demands, and other communications required or permitted under this Agreement shall be in writing. A notice, request, demand, or other communication shall be deemed to have been duly given, made and received (a) when personally delivered, or (b) on the day specified for delivery when deposited with a courier service such as Federal Express for delivery to the intended addressee, or (c) three business days following the day when deposited in the Unite States mail, registered or certified mail, postage prepaid, return receipt requested, addressed as set forth below:

If to HIE:	If to Participant:
_____	_____
_____	_____

_____	_____
_____	_____
Attn: _____	Attn:_____

Nothing in this section shall prevent the parties from communicating via electronic mail, telephone, facsimile, or other forms of communication for the routine administration of the Exchange.

12.7 No Agency. HIE provides the Exchange services to Participating Health Care Providers but does not act for Participating Health Care Providers.

12.8 No Relationship between Participating Health Care Providers; No Third Party Rights. Nothing in this Agreement confer any rights or remedies under this Agreement on any persons other than HIE and Participant, and nothing in this Agreement is intended to create a contractual relationship among Participating Health Care Providers, except to the extent that each such Participating Health Care Provider is a beneficiary under Section 8. Nothing in this Agreement will give any third party, including other Participating Health Care Providers, any right of subrogation or action against any party to this Agreement.

For the AHCCCS HIE:

[12.9 The parties agree to be bound by applicable state and federal rules and laws governing Equal Employment Opportunity and Non-Discrimination.]

[12.10 This Agreement is subject to cancellation pursuant to the provisions of A.R.S. 38-511 regarding Conflict of Interest.]

EXHIBIT B

HIE INFORMATION SECURITY REQUIREMENTS

In addition to any obligations set forth in the Agreement and HIE security Policies and Standards, Participant will observe the following requirements. HIE may amend or supplement these requirements on written notice to Participant.

1. Each of Participant's servers connecting to the HIE gateway will comply with HIE's authentication requirements, including certificate policies.

2. Participant will implement authentication of each Authorized User at the point of access and will implement password policies based on prevailing industry standards and HIE policies. Participant may elect to implement stronger authentication (e.g. token)at its discretion.

3. Participant will authorize each Authorized User based on the permitted use of the HIE Exchange. Participant will impose appropriate sanctions for members of its workforce that violate security policies or make improper use of the Exchange, including revocation of an Authorized User's authorization to access the Exchange as may be appropriate under the circumstances

4. Participant will maintain access logs that capture end use identification information.

5. Participant will implement SSL encryption and authentication, using certificates approved by HIE.

6. Participant will implement message-level security using WS-Security or other security technology acceptable to HIE.

7. Participant will implement Role Based Access Controls based on roles approved by HIE and pursuant to Exchange policies.

8. Participant will implement firewalls and intrusion detection per industry standards and Exchange policies.

9. Participant will implement other safeguards to protect servers based on **SANS recommendations.**

10. Participant will perform periodic automated and random manual review and verification of audit logs for both operational monitoring and system security as required by Exchange policies.

EXHIBIT C
BUSINESS ASSOCIATE AGREEMENT

HIE and Participant agree to the terms and conditions of this Business Associate Agreement in order to comply with the use and handling of Protected Health Information ("PHI") under the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Rule") and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Rule"), both as amended from time to time. Unless otherwise provided, all capitalized terms in this Agreement will have the same meaning as provided under the Privacy Rule and Security Rule.

For purposes of this Business Associate Agreement, Protected Health Information ("PHI") or Electronic Protected Health Information ("EPHI") includes only individually identifiable health information handled by HIE that is provided to the Exchange by Participant.

1. USES AND DISCLOSURES OF PHI: HIE will use or disclose PHI only for those purposes necessary to perform Services under the Agreement, or as otherwise expressly permitted in the Agreement or this Business Associate Agreement, or as required by law, and will not further use or disclose PHI. HIE agrees that anytime it provides PHI to a subcontractor or agent to perform Services, HIE first will enter into a contract with such subcontractor or agent that contains the same terms, conditions, and restrictions on the use and disclosure of PHI as contained in this Agreement.

2. HIE USE OR DISCLOSURE OF PHI FOR ITS OWN PURPOSES: HIE may use or disclose PHI for Business Associate's management and administration, or to carry out Business Associate's legal responsibilities. HIE may disclose PHI to a third party for such purposes if: (1) The disclosure is required by law; or (2) HIE secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) use or disclose the PHI only as required by law or for the purposes for which it was disclosed to the recipient; and (iii) notify the HIE of any breaches in the confidentiality of the PHI. HIE also may aggregate the PHI with other PHI in its possession or otherwise de-identify PHI according to the requirements of 45 C.F.R. §164.514(b).

3. SAFEGUARDS: HIE will implement and maintain appropriate safeguards to prevent any use or disclosure of PHI for purposes other than those permitted by this Business Associate Agreement. HIE also will implement administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any EPHI that HIE creates, receives, maintains, and transmits on behalf of Participant.

4. UNAUTHORIZED USES OR DISCLOSURES: HIE will report in writing to Participant any use or disclosure of PHI for purposes other than those permitted by this Business Associate Agreement within 15 business days of HIE learning of such use or disclosure. HIE also will report any Security Incident involving EPHI within 15 business days of Business Associate's learning of such Security Incident. HIE will establish procedures for mitigating, to the greatest extent possible, any harm to Participant's patients from any unauthorized use or disclosure of PHI.

[Alternative provision that manages the "Security Incident" reporting with more specificity: HIE will report to Participant any successful unauthorized access, use, disclosure, modification, or

destruction of EPHI or interference with system operations in an information system containing EPHI of which HIE becomes aware within 15 business days of Business Associate's learning of such event. HIE will report the aggregate number of unsuccessful, unauthorized attempts to access, use, disclose, modify, or destroy EPHI or interfere with system operations in an information system containing EPHI, of which HIE becomes aware, provided that such reports will be provided only as frequently as the parties mutually agree, but no more than once per month. If the definition of "Security Incident" under the Security Rule is amended to remove the requirement for reporting "unsuccessful" attempts to use, disclose, modify or destroy EPHI, HIE will cease reporting unauthorized attempts as of the effective date of such amendment.]

5. INDIVIDUAL ACCESS TO PHI: If an individual makes a request to HIE for access to PHI, HIE will within 10 business days forward such request in writing to Participant. Participant will be responsible for making all determinations regarding the grant or denial of an individual's request for PHI and HIE will make no such determinations.

6. AMENDMENT OF PHI: If an individual makes a request to HIE for amendment of PHI, HIE will within 10 business days forward such request in writing to Participant. Participant will be responsible for making all determinations regarding amendments to PHI and HIE will make no such determinations.

7. ACCOUNTING OF DISCLOSURES OF PHI: If an individual makes a request to HIE for an accounting of disclosures of PHI, HIE will within 10 business days forward such request in writing to Participant. Participant will be responsible for preparing and delivering the accounting to the individual. Upon request, HIE will make available to Participant information about Business Associate's disclosures of PHI, if any, that must be included to respond to individual requests for accounting of disclosures of PHI.

8. ACCESS TO BOOKS AND RECORDS: HIE will make its internal practices, books and records on the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services to the extent required for determining Participant's compliance with the Privacy Rule. Notwithstanding this provision, no attorney-client, accountant-client or other legal privilege will be deemed waived by HIE or Participant as a result of this Section.

9. TERMINATION: Participant may terminate the Agreement upon written notice to HIE if HIE breaches a material term of this Business Associate Agreement and HIE fails to cure the breach within thirty days of the date of notice of the breach.

10. RETURN OR DESTRUCTION OF PHI: Participant understands that PHI is integrated into a permanent longitudinal medical record that reflects the care of patients by Participant, HIE, and other providers. As such, it is not feasible for HIE to return or destroy PHI upon termination of the Agreement. HIE agrees to follow the provisions of this Business Associate Agreement for as long as it retains PHI, and will limit any further use or disclosure of PHI to those purposes allowed under this Business Associate Agreement, until such time as HIE either returns or destroys the PHI.

PROJECT ADENDUM NO. 1

Project Name	
Data to be Exchanged	
Permitted Uses	
Permitted Users	
Specific Safeguards and Privacy Requirements	
Licensed Software	
Certification Requirements	
Disclaimer	
Indemnification	
Confidential Information	
Definitions for Project Addendum No. 1	